Carnegie Mellon Software Engineering Institute

OCTAVE®-S Implementation Guide, Version 1.0

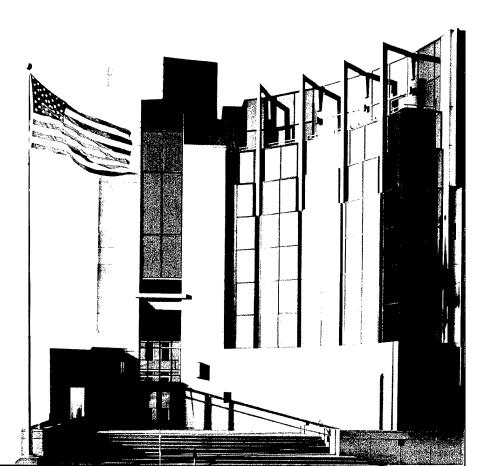
Volume 9: Strategy and Plan Worksheets

Christopher Alberts Audrey Dorofee James Stevens Carol Woody

January 2005

DISTRIBUTION STATEMENT A

Approved for Public Release Distribution Unlimited



HANDBOOK CMU/SEI-2003-HB-003



Pittsburgh, PA 15213-3890

OCTAVE®-S Implementation Guide, Version 1.0

Volume 9: Strategy and Plan Worksheets

CMU/SEI-2003-HB-003

Christopher Alberts Audrey Dorofee James Stevens Carol Woody

January 2005

Networked Systems Survivability Program

Unlimited distribution subject to the copyright.

20050322 131

This report was prepared for the

SEI Joint Program Office ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER

Christos Scondras Chief of Programs, XPK

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

Copyright 2005 by Carnegie Mellon University.

® OCTAVE is registered in the U.S. Patent & Trademark Office by Carnegie Mellon University.

SM Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use. Requests for permission to reproduce this document or prepare derivative works of this document for external and commercial use should be addressed to the SEI Licensing Agent.

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

Ab	out This Document	V
Abs	stract	vii
1	Introduction	1
2	Notes and Recommendations Worksheet	3
3	Action List Worksheet	13
4	Protection Strategy Worksheet	23
5	Mitigation Activities Guide	83
6	Mitigation Plan Worksheet	115
7	Next Steps Worksheet	129

List of Tables

Table 1:	Worksheets Provided in This Workbook
----------	--------------------------------------

About This Document

This document is Volume 9 of the *OCTAVE-S Implementation Guide*, a 10-volume handbook supporting the OCTAVE-S methodology. This volume contains worksheets to record the organization's current and desired protection strategies and the risk mitigation plans.

The volumes in this handbook are

- Volume 1: Introduction to OCTAVE-S This volume provides a basic description of OCTAVE-S and advice on how to use the guide.
- Volume 2: Preparation Guidelines This volume contains background and guidance for preparing to conduct an OCTAVE-S evaluation.
- Volume 3: Method Guidelines This volume includes detailed guidance for each OCTAVE-S activity.
- Volume 4: Organizational Information Workbook This volume provides worksheets for all organizational-level information gathered and analyzed during OCTAVE-S.
- Volume 5: Critical Asset Workbook for Information This volume provides worksheets to document data related to critical assets that are categorized as information.
- Volume 6: Critical Asset Workbook for Systems This volume provides worksheets to
 document data related to critical assets that are categorized as systems.
- Volume 7: Critical Asset Workbook for Applications This volume provides worksheets to
 document data related to critical assets that are categorized as applications.
- Volume 8: Critical Asset Workbook for People This volume provides worksheets to
 document data related to critical assets that are categorized as people.
- Volume 9: Strategy and Plan Workbook This volume provides worksheets to record the current and desired protection strategy and the risk mitigation plans.
- Volume 10: Example Scenario This volume includes a detailed scenario illustrating a completed set of worksheets.

Abstract

The Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE®) approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organization's business and security processes, so it will be able to conduct all activities by itself.

1 Introduction

This document contains the Operationally Critical Threat, Asset, and VulnerabilitySM (OCTAVE®)-S worksheets related to the organization's strategy development and planning activities.

Table 1 provides a brief introduction to the contents of this workbook, using activity step numbers as a key. For more details about how to complete each step, refer to the OCTAVE®-S Method Guidelines, which can be found in Volume 3 of the OCTAVE®-S Implementation Guide.

Table 1: Worksheets Provided in This Workbook

Step	Description	Worksheet	Activity	Pages
	Document notes and recommendations identified during each step.	Notes and Recommendations	All Phases All Processes All Activities	3-12
	Document action items identified during each step.	Action List	All Phases All Processes All Activities	13-22
Step 25	Transfer the stoplight status of each security practice area to the corresponding area of the <i>Protection Strategy worksheet</i> . For each security practice area, identify your organization's current approach for addressing that area.	Protection Strategy	Phase 3 Process S5 S5.1 Describe Current Protection Strategy	23-82

OCTAVE is registered in the United States Patent and Trademark Office by Carnegie Mellon University.

Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

Introduction OCTAVE-S V1.0

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 28	Develop mitigation plans for each security practice area selected during Step 27. As you complete this step, if you have difficulty coming up with potential mitigation activities for a security practice area, review examples of mitigation activities for that area in the Mitigation Activities Guide.	Mitigation Plan	Phase 3 Process S5 S5.3 Develop Risk Mitigation Plans	115-128
Step 29	Determine whether your mitigation plans affect your organization's protection strategy. Record any changes on the Protection Strategy worksheet.	Protection Strategy	Phase 3 Process S5 S5.4 Identify Changes to Protection Strategy	23-82
	Next, review the protection strategy, including proposed changes. Determine whether you intend to make any additional changes to the protection strategy. Record any additional changes on the <i>Protection Strategy worksheet</i> .			
Step 30	Determine what your organization must do to implement the results of this evaluation and improve its security posture.	Next Steps	Phase 3 Process S5 S5.5 Identify Next Steps	129-132

2 Notes and Recommendations Worksheet

All Phases
All Processes
All Activities

Throughout Evaluation

Document notes and recommendations identified during each step.

Note		
What notes do you want		For which step is this note relevant?
Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.		
		Step

Note		
What notes do you want to record? Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.		For which step is this note relevant?
		Step
·		

	Recommendation	
What recommendations do you want to record?		For which step is this recommendation relevant?
		Step
·		

		_
	Recommendation	
What recommendations do you want to record?		For which step is this recommendation relevant?
•		Step
	·	
·		

Note		
What notes do you want		For which step is this note relevant?
Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.		
	·	Step

step is elevant?
·

	Recommendation	
What recommendations do you want to record?		For which step is this recommendation relevant?
		Step

	Recommendation	·
What recommendations do you want to record?		For which step is this recommendation relevant?
		Step
·		
•		

Note		
What notes do you want to reco		For which step is this note relevant?
Is there a recommendation associately corresponding recommendation	ociated with this note? If yes, document it in the as box.	mis note retermin.
		Step

Note		
What notes do you want Is there a recommendation	on associated with this note? If yes, document it in the	For which step is this note relevant?
corresponding recomme	ndations box.	
		Step

Recommendation	·
	For which step is this recommendation relevant?
	Step
	Recommendation

	Recommendation	
What recommendations do you want to record?		For which step is this recommendation relevant?
		Step
·		

Note		•
What notes do you want to		For which step is this note relevant?
Is there a recommendation corresponding recommend	n associated with this note? If yes, document it in the dations box.	
		Step
	·	

Note		
What notes do you want Is there a recommendation corresponding recommendations.	on associated with this note? If yes, document it in the	For which step is this note relevant?
		Step

	Recommendation	
What recommendations do you want to record?		For which step is this recommendation relevant?
		Step

	Recommendation	
What recommendations do you want to record?		For which step is this recommendation relevant?
		Step
		<u>.</u>

3 Action List Worksheet

All Processes All Activities

Throughout Evaluation

Document action items identified during each step.

Action Item	
What actions do you intend to take? Assign an identification number to each action item.	For which step is this action item relevant?
	Step
	What actions do you intend to take?

Action Item	
What actions do you intend to take? Assign an identification number to each action item.	For which step is this action item relevant?
	Step
,	
	What actions do you intend to take? Assign an identification number to each action item.

v		Action Item
	What additional information do you want to document for each a	ction item?
	Record additional information below.	
Responsibility:	Who is responsible for completing the action item?	
		,
Completion Date:	By when must the action item be completed?	
Additional Support:	What additional support (by management or others) is required t action item?	o complete the

	Action Item
	What additional information do you want to document for each action item?
	Record additional information below.
Responsibility:	Who is responsible for completing the action item?
Completion Date:	By when must the action item be completed?
Additional Support:	What additional support (by management or others) is required to complete the action item?

Action Item	
What actions do you intend to take? Assign an identification number to each action item.	For which step is this action item relevant?
	Step
	What actions do you intend to take?

Action Item	
What actions do you intend to take? Assign an identification number to each action item.	For which step is this action item relevant?
	Step
	What actions do you intend to take?

	Action Item	
	What additional information do you want to document for each action item?	
	Record additional information below.	
Responsibility:	Who is responsible for completing the action item?	
Completion Date:	By when must the action item be completed?	
Additional Support:	What additional support (by management or others) is required to complete the action item?	

		Action Item
	What additional information do you want to document for each action item?	
	Record additional information below.	
Responsibility:	Who is responsible for completing the action item?	
		·
G welster Deter	By when must the action item be completed?	
Completion Date:	By when must the action tiem be completed:	,
Additional	What additional support (by management or others) is required to action item?	o complete the
Support:	action tiem:	·

Action Item	
What actions do you intend to take? Assign an identification number to each action item.	For which step is this action item relevant?
	Step
- -	
	i.
	What actions do you intend to take?

	Action Item	
	What actions do you intend to take? Assign an identification number to each action item.	For which step is this action item relevant?
ID#		Step
	<u> </u> .	

What additional information do you want to document for each action item?

Record additional information below.

Who is responsible for completing the action item?

Completion Date:

By when must the action item be completed?

What additional support (by management or others) is required to complete the action item?

	Action Item
	What additional information do you want to document for each action item?
	Record additional information below.
Responsibility:	Who is responsible for completing the action item?
Completion Date:	By when must the action item be completed?
Additional Support:	What additional support (by management or others) is required to complete the action item?

	Action Item	
	What actions do you intend to take? Assign an identification number to each action item.	For which step is this action item relevant?
ID#		Step

	Action Item	
	What actions do you intend to take? Assign an identification number to each action item.	For which step is this action item relevant?
ID#		Step
	·	

	Action Item	
	What additional information do you want to document for each action item?	
	Record additional information below.	
Responsibility:	Who is responsible for completing the action item?	
Completion Date:	By when must the action item be completed?	
Additional Support:	What additional support (by management or others) is required to complete the action item?	
Support		

	Action Item
What additional information do you want to document for each action item?	
cord additional information below.	
no is responsible for completing the action item?	
By when must the action item be completed?	
hat additional support (by management or others) is required to them?	to complete the
	cord additional information below. no is responsible for completing the action item? when must the action item be completed? hat additional support (by management or others) is required

4 Protection Strategy Worksheet

Phase 3
Process S5
Activity S5.1

Step 25

Transfer the stoplight status of each security practice area to the corresponding area of the *Protection Strategy worksheet*.

For each security practice area, identify your organization's current approach for addressing that area.

Phase 3
Process S5
Activity S5.4

Step 29

Determine whether your mitigation plans affect your organization's protection strategy. Record any changes on the *Protection Strategy worksheet*.

Next, review the protection strategy, including proposed changes. Determine whether you intend to make any additional changes to the protection strategy. Record any additional changes on the *Protection Strategy worksheet*.

1. Security Awareness and Training		Stoplight Status
------------------------------------	--	------------------

- Step 25: How formal is your organization's training strategy?
- Step 29: Will any mitigation activities change your training strategy?

 Do you want to make any additional changes to your training strategy?

Training Strategy		Step 25		Step 29	
The organization has a documented training strategy that includes security awareness training and security-related training for supported technologies.			Current		Change
The organization has an informal and undocumented training strategy.		۵	Current		Change
			Current		Change

Step 25: How often is security awareness training provided?

Step 29: Will any mitigation activities change how often security awareness training is provided?

Do you want to make any additional changes to how often security awareness training is provided?

Security Awareness Training	Step 25		Step 29	
Periodic security awareness training is provided for all employeestime(s) every years.	<u> </u>	Current		Change
Security awareness training is provided for new staff members as part of their orientation activities.		Current		Change
The organization does not provide security awareness training. Staff members learn about security issues on their own.	0	Current		Change
	۵	Current		Change

1. Security Awareness and Training

Step 25: To what extent are IT staff members required to attend security-related training?

Step 29: Will any mitigation activities change the requirement for attending security-related training?

Do you want to make any additional changes to the requirement for attending security-related training?

ecurity-Related Training for Supported Technologies		Step 25		Step 29	
Information technology staff members are required to attend security-related training for any technologies that they support.	0	Current	۵	Change	
Information technology staff members can attend security-related training for any technologies that they support if they request it.		Current		Change	
The organization generally does not provide opportunities for information technology staff members to attend security-related training for supported technologies. Information technology staff members learn about security-related issues on their own.		Current	0	Change	
	0	Current		Change	

Step 25: How formal is your organization's mechanism for providing periodic security updates?

Step 29: Will any mitigation activities change your mechanism for providing periodic security updates?

Do you want to make any additional changes to your mechanism for providing periodic security updates?

Periodic Security Updates		Step 25		Step 29	
The organization has a formal mechanism for providing staff members with periodic updates/bulletins about important security issues.			Current		Change
The organization does not have a mechanism for providing staff members with periodic updates/bulletins about important security issues.		Q	Current		Change
		u	Current	0	Change
					i

1. Security Awareness and Training

Step 29: Will any mitigation activities change your mechanism for verifying that staff rec Do you want to make any additional changes to your mechanism for verifying th	at staff	receives tra	ining.	?	
Fraining Verification	Sto	Step 25		Step 29	
The organization has formal mechanisms for tracking and verifying that staff members receive appropriate security-related training.	0	Current	0	Change	
The organization has informal mechanisms for tracking and verifying that staff members receive appropriate security-related training.	٥	Current	0	Change	
The organization has no mechanisms for tracking and verifying that staff members receive appropriate security-related training.	0	Current	٥	Change	
		Current		Change	
Step 25: What additional characteristic of your current approach to security awareness	and trai	ining do you	ı wanı	10	
record? Step 29: Will any mitigation activities change this characteristic? Do you want to make any additional changes to this characteristic?		ining do you		ep 29	
record? Step 29: Will any mitigation activities change this characteristic?					
record? Step 29: Will any mitigation activities change this characteristic? Do you want to make any additional changes to this characteristic?		ep 25	St	ер 29	
record? Step 29: Will any mitigation activities change this characteristic? Do you want to make any additional changes to this characteristic?		ep 25 Current	St	ep 29 Change	
record? Step 29: Will any mitigation activities change this characteristic? Do you want to make any additional changes to this characteristic?	St	ep 25 Current	St	ep 29 Change	

Stoplight Status

2.	Security	Strategy
----	-----------------	----------

Stoplight Status

Step 25: How formal is your organization's mechanism for integrating security and business strategies?

Step 29: Will any mitigation activities change your mechanism for integrating security and business strategies?

Do you want to make any additional changes to your mechanism for integrating security and business strategies?

Business and Security Strategy Integration	Ste	ep 25	Ste	р 29
The organization has formal mechanisms for integrating • security considerations into business strategies		Current		Change
 security considerations into outsiness strategies and goals into security strategies and policies 				
The organization has informal mechanisms for integrating • security considerations into business strategies		Current		Change
 security considerations into business strategies and goals into security strategies and policies 				
The organization has no mechanisms for integrating • security considerations into business strategies		Current		Change
 business strategies and goals into security strategies and policies 				
	۵	Current		Change

Step 25: How formal are your organization's security strategies, goals, and objectives?

Step 29: Will any mitigation activities change your security strategies, goals, and objectives?

Do you want to make any additional changes to your security strategies, goals, and objectives?

Do you want to make any adattional changes to your security extragally	Sto	ep 25	Ste	р 29
Documented Strategies				
The organization has documented security strategies, goals, and objectives.		Current		Change
The organization has a partial set of documented security strategies, goals, and objectives. Some aspects of security strategies, goals, and objectives are informal and undocumented.	0	Current	O	Change
The organization has informal and undocumented security strategies, goals, and objectives.	0	Current		Change
——————————————————————————————————————		Current		Change

2. Security Strategy

- Step 25: To what extent does your security awareness training program include information about the organization's security strategy?
- Step 29: Will any mitigation activities change the content of your security awareness training to include strategy information?

 Do you want to make any additional changes to the content of your security awareness training?

Staff Awareness	Ste	ep 25	Ste	ep 29
The organization's security awareness training program includes information about the organization's security strategy. This training is provided for all employeestime(s) every years.	Q	Current		Change
The organization's security awareness training program includes information about the organization's security strategy. This training is provided for new staff members as part of their orientation activities.	0	Current		Change
The organization's security awareness training program does not include information about the organization's security strategy. Staff members learn about the organization's security strategy on their own.		Current		Change
	Q	Current		Change

Step 25: What additional characteristic of your current approach to security strategy do you want to record?

Step 29: Will any mitigation activities change this characteristic?

Do you want to make any additional changes to this characteristic?

Other:	Step 25	Step 29
	☐ Current	☐ Change
	☐ Current	☐ Change
	☐ Current	☐ Change

3.	Security	Management
\sim	December	1,14,14,14

Stoplight Status	toplight Status	
------------------	-----------------	--

Step 25: To what extent are security roles and responsibilities formally defined?

Step 29: Will any mitigation activities change the extent to which security roles and responsibilities are formally defined?

Do you want to make any additional changes to how security roles and responsibilities are formally defined?

Sto	ep 25	Sto	ep 29
۵	Current		Change
0	Current		Change
0	Current		Change
۵	Current		Change
		□ Current □ Current	Current Curren

Step 25: To what extent is security formally factored into your organization's budget?

Step 29: Will any mitigation activities change how security is formally factored into your organization's budget?

Do you want to make any additional changes to how security is formally factored into your organization's budget?

Funding	Ste	ep 25	Ste	ep 29
The organization's budget has a distinct line item for information security activities. The funding level is determined based on a formal assessment of the organization's information security risks.	0	Current	0	Change
The organization's budget has a distinct line item for information security activities. The funding level is determined using informal processes.	0	Current		Change
The organization's budget explicitly includes information security activities under the line item for information technology (IT). The funding level is determined based on a formal assessment of the organization's information security risks.		Current	0	Change
The organization's budget explicitly includes information security activities under the line item for information technology. The funding level is determined using informal processes.		Current		Change
Neither the organization's budget nor the IT department's budget explicitly includes funding for information security activities.	0	Current		Change
		Current		Change

3. Security Management

Step 25: How formal are your organization's security-related human resource procedures?

Step 29: Will any mitigation activities change your security-related human resource procedures?

Do you want to make any additional changes to your security-related human resource procedures?

Human Resource Procedures		Ste	ep 25	Ste	р 29
The organization has formally defined procedures for includ considerations in the organization's hiring (e.g., background termination (e.g., removing access to all systems and inform	checks) and		Current		Change
The organization has some formally defined procedures for considerations in the organization's hiring (e.g., background termination (e.g., removing access to all systems and inform Some procedures in this area are informal and undocumente	checks) and ation) processes.		Current		Change
The organization has informal and undocumented procedure security considerations in the organization's hiring (e.g., bactermination (e.g., removing access to all systems and information (e.g., removing access to all systems and elementation (e.g., removing access to all systems acc	ckground checks) and	٥	Current		Change
		۵	Current	0	Change

Step 25: How formal is your organization's process for managing information security risk?

Step 29: Will any mitigation activities change your process for managing information security risk?

Do you want to make any additional changes to your process for managing information security risk?

Risk Management	St	ep 25	Ste	ep 29
The organization has a formally defined process for assessing a information security risks.	nd managing its	Current	٦	Change
The organization has a formally defined process for assessing it security risks. The process for managing information security riand undocumented.	ts information isks is informal	Current		Change
The organization has an informal and undocumented approach managing its information security risks.	for assessing and	Current		Change
		Current	۵	Change

3.	Security	Management
J.	Security	MINIMPONTON

Stopingin Status	Stoplight Status	
------------------	------------------	--

- Step 25: To what extent does your security-awareness training program include information about the organization's security management process?
- Step 29: Will any mitigation activities change the content of your security awareness training to include security management information?

 Do you want to make any additional changes to the content of your security awareness training?

Staff Awareness	Sto	ep 25	Ste	ep 29
The organization's security-awareness training program includes information about the organization's security management process. This training is provided for all employeestime(s) every years.	٥	Current	0	Change
The organization's security-awareness training program includes information about the organization's security management process. This training is provided for new staff members as part of their orientation activities.		Current		Change
The organization's security-awareness training program does not include information about the organization's security management process. Staff members learn about security management on their own.	۵	Current		Change
•	0	Current		Change

Step 25: How formal is your organization's mechanism for providing managers with security-related information?

Step 29: Will any mitigation activities change how security-related information is provided to managers?

Do you want to make any additional changes to how security-related information is provided to managers?

Management Awareness	Sto	ep 25	Ste	ep 29
The organization has a formal mechanism for providing managers with summaries of important security-related information.		Current		Change
The organization has an informal and undocumented mechanism for providing managers with summaries of important security-related information.	۵	Current	۵	Change
The organization has no mechanism for providing managers with summaries of important security-related information.	0	Current		Change
	0	Current	0	Change

3. Security Management

Step 25: What additional characteristic of your current approach to security management do you want to record?

Step 29: Will any mitigation activities change this characteristic?

Do you want to make any additional changes to this characteristic?

Other:	Step 25	Step 29		
	☐ Current	☐ Change		
	☐ Current	☐ Change		
	☐ Current	☐ Change		

4.	Security	Policies	and	Regulations
----	----------	-----------------	-----	-------------

Step 25: To what extent are your organization's security-related policies formally documented?

Step 29: Will any mitigation activities change the extent to which your security-related policies are formally documented?

Do you want to make any additional changes to the formality and documentation of your security-related policies?

Documented Policies	Ste	p 25	Ste	ep 29
The organization has a comprehensive set of formally documented security-related policies.		Current		Change
The organization has a partial set of formally documented security-related policies. Some security-related policies are informal and undocumented.		Current		Change
The organization's security-related policies are informal and undocumented.		Current		Change
		Current		Change

Step 25: How formal is your organization's mechanism for creating and updating its security-related policies?

Step 29: Will any mitigation activities change how security-related policies are created and updated?

Do you want to make any additional changes to how security-related policies are created and updated?

Policy Management	Sto	ep 25	Ste	р 29
The organization has a formal mechanism for creating and updating its security-related policies.		Current	0	Change
The organization has a formal mechanism for creating its security-related policies. The organization has an informal and undocumented mechanism for updating its security-related policies.		Current		Change
The organization has an informal and undocumented mechanism for creating and updating its security-related policies.	0	Current	0	Change
		Current	۵	Change

4. Security Policies and Regulations

Step 25: How formal are your organization's procedures for enforcing its security-related policies?

Step 29: Will any mitigation activities change how security-related policies are enforced?

Do you want to make any additional changes to how security-related policies are enforced?

Policy Enforcement	Step 25	Step 29
The organization has formal procedures for enforcing its security-related policies. Enforcement procedures are consistently followed.	☐ Current	☐ Change
The organization has formal procedures for enforcing its security-related policies. Enforcement procedures are inconsistently followed.	☐ Current	☐ Change
The organization has informal and undocumented procedures for enforcing its security-related policies.	☐ Current	☐ Change
	☐ Current	☐ Change

- Step 25: To what extent does your security-awareness training program include information about the organization's security policies and regulations?
- Step 29: Will any mitigation activities change the content of your security awareness training to include security policy and regulation information?

 Do you want to make any additional changes to the content of your security awareness training?

Step 29 Step 25 Staff Awareness The organization's security-awareness training program includes information ☐ Current ☐ Change about the organization's security policies and regulations. This training is ___time(s) every _ provided for all employees __ The organization's security-awareness training program includes information ☐ Current ☐ Change about the organization's security policies and regulations. This training is provided for new staff members as part of their orientation activities. The organization's security-awareness training program does not include ☐ Current ☐ Change information about the organization's security policies and regulations. Staff members learn about security policies and regulations on their own. ☐ Current ☐ Change

tep 25: How formal are your organization's procedures for complying with security-related to the parties with security tep 29: Will any mitigation activities change how your organization complies with security regulations?				<u> </u>
	d poli	cies and reg	zulatio	ons?
regulations? Do you want to make any additional changes to how your organization complies wi regulations?				cies and
olicy and Regulation Compliance	Ste	p 25	Ste	p 29
The organization has formal procedures for complying with information security olicies, applicable laws and regulations, and insurance requirements.		Current		Change
The organization has formal procedures for complying with certain information ecurity policies, applicable laws and regulations, and insurance requirements.	0	Current	<u> </u>	Change
The organization has informal and undocumented procedures for complying with information security policies, applicable laws and regulations, and insurance equirements.	0	Current		Change
		Current		Change
Step 25: What additional characteristic of your current approach to security policies and re record? Step 29: Will any mitigation activities change this characteristic? Do you want to make any additional changes to this characteristic?	egula:	tions do you	! want	to
20 your man to many and				
Other:	St	ep 25	Sto	ep 29
	St	Current	Sto	ep 29 Change

Stoplight Status

· Protection Strategy Worksheet

Collaborative Security Management Stoplight Status				
Step 25: How formal are your organization's policies and procedures for protecting information collaborators and partners?				
Step 29: Will any mitigation activities change the policies and procedures for protecting infecollaborators and partners? Do you want to make any additional changes to the policies and procedures for procedures for procedures working with collaborators and partners?				
Collaborators and Partners	Ste	ер 25	Ste	p 29
The organization has documented policies and procedures for protecting information when working with collaborators and partners.	0	Current	٥	Change
The organization has documented policies and procedures for protecting certain information when working with collaborators and partners. The organization has informal and undocumented policies and procedures for protecting other types of information when working with collaborators and partners.		Current	0	Change
The organization has informal and undocumented policies and procedures for protecting information when working with collaborators and partners.		Current	0	Change
		Current	0	Change
Step 25: How formal are your organization's policies and procedures for protecting informations and subcontractors? Step 29: Will any mitigation activities change the policies and procedures for protecting ingo contractors and subcontractors? Do you want to make any additional changes to the policies and procedures for procedures for procedures working with contractors and subcontractors? Contractors and Subcontractors	forma otecti	ation when v	workin tion w	ng with
			П	Change
The organization has documented policies and procedures for protecting information when working with contractors and subcontractors.	U —	Current	u	Change
The organization has documented policies and procedures for protecting certain information when working with contractors and subcontractors. The organization has informal and undocumented policies and procedures for protecting other types of information when working with contractors and subcontractors.	0	Current	0	Change
The organization has informal and undocumented policies and procedures for protecting information when working with contractors and subcontractors.		Current	· 🗖	Change

☐ Current ☐ Change

5. Collaborative Security Management

- Step 25: How formal are your organization's policies and procedures for protecting information when working with service providers?
- Step 29: Will any mitigation activities change the policies and procedures for protecting information when working with service providers?

 Do you want to make any additional changes to the policies and procedures for protecting information when working with service providers?

Service Providers	Ste	ep 25	Step 29	
The organization has documented policies and procedures for protecting information when working with service providers.		Current		Change
The organization has documented policies and procedures for protecting certain information when working with service providers. The organization has informal and undocumented policies and procedures for protecting other types of information when working with service providers.	0	Current	0	Change
The organization has informal and undocumented policies and procedures for protecting information when working with service providers.	۵	Current	0	Change
	0	Current		Change

- Step 25: To what extent does your organization formally communicate its information protection requirements to third parties?
- Step 29: Will any mitigation activities change how your organization communicates its information protection requirements to third parties?

 Do you want to make any additional changes to how your organization communicates its information protection requirements to third parties?

Requirements	Ste	ep 25	Sto	ep 29
The organization documents information protection requirements and explicitly communicates them to all appropriate third parties.		Current		Change
The organization informally communicates information protection requirements to all appropriate third parties.	٥	Current		Change
The organization does not communicate information protection requirements to third parties.	0	Current	0	Change
		Current	٥	Change

5.	Collaborative	Security	Management

Stoplight Status	
------------------	--

- Step 25: To what extent does your organization verify that third parties are addressing information protection requirements?
- Step 29: Will any mitigation activities change verification mechanisms?

 Do you want to make any additional changes to verification mechanisms?

Verification	Sto	ep 25	Sto	ер 29
The organization has formal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.		Current	0	Change
The organization has informal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.		Current	0	Change
The organization has no mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.	Q	Current		Change
	0	Current	0	Change

- Step 25: To what extent does your security-awareness training program include information about collaborative security management?
- Step 29: Will any mitigation activities change the content of your security awareness training to include information about collaborative security management?

 Do you want to make any additional changes to the content of your security awareness training?

Step 29 Step 25 Staff Awareness The organization's security-awareness training program includes information Current Change about the organization's collaborative security management policies and procedures. This training is provided for all employees _____time(s) every years. The organization's security-awareness training program includes information Current ☐ Change about the organization's collaborative security management policies and procedures. This training is provided for new staff members as part of their orientation activities. The organization's security-awareness training program does not include ☐ Current ☐ Change information about the organization's collaborative security management policies and procedures. Staff members learn about collaborative security management policies and procedures on their own. ☐ Change ☐ Current

5. Collaborative Security Management

- Step 25: What additional characteristic of your current approach to collaborative security management do you want to record?
- Step 29: Will any mitigation activities change this characteristic?

 Do you want to make any additional changes to this characteristic?

Other:	Step 25	Step 29
	☐ Current	☐ Change
	☐ Current	☐ Change
	☐ Current	☐ Change

6.	Contingency	Planning/Disaster	Recovery
----	-------------	-------------------	----------

Stoplight Status	
300F8	

- Step 25: To what extent has an analysis of operations, applications, and data criticality been performed?
- Step 29: Will any mitigation activities change the extent to which business operations are analyzed?

 Do you want to make any additional changes to business operations analysis?

Business Operations Analysis		Ste	ep 25	Ste	ep 29
An analysis of operations, applications, and data criticality h	as been performed.		Current		Change
A partial analysis of operations, applications, and data critica performed.	ality has been	0	Current		Change
An analysis of operations, applications, and data criticality h performed.	as not been	0	Current	۵	Change
		0	Current	0	Change

- Step 25: To what extent has your organization documented its contingency plans?
- Step 29: Will any mitigation activities change how contingency plans are documented?

 Do you want to make any additional changes to contingency plan documentation?

Documented Plans	Sto	ep 25	Sto	ер 29
The organization has documented business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.		Current		Change
The organization has partially documented business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies. Some aspects of the plans are informal and undocumented.		Current	٥	Change
The organization has informal and undocumented business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	0	Current	0	Change
	0	Current	0	Change

6. Contingency Planning/Disaster Recovery

Step 25: To what extent has your organization tested its contingency plans?

Step 29: Will any mitigation activities change how contingency plans are tested?

Do you want to make any additional changes to contingency plan testing?

Tested Plans	Ste	ep 25	Ste	ер 29
The organization has formally tested its business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.		Current		Change
The organization has informally tested its business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.		Current	0	Change
The organization has not tested its business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.		Current	0	Change
		Current		Change

Step 25: To what extent is physical and electronic access to critical information formally factored into contingency plans?

Step 29: Will any mitigation activities change the extent to which information access is formally factored into contingency plans?

Do you want to make any additional changes to how information access is formally factored into contingency plans?

Information Access	Sto	ep 25	Sto	ер 29
Physical and electronic access to critical information is formally factored into the organization's contingency, disaster recovery, and business continuity plans.		Current		Change
Physical and electronic access to some critical information is formally factored into the organization's contingency, disaster recovery, and business continuity plans. Other types of critical information are not formally factored into the plans.	0	Current	0	Change
Physical and electronic access to critical information is not formally factored into the organization's contingency, disaster recovery, and business continuity plans.		Current	0	Change
		Current	۵	Change

6. Contingency Planning/Disaster Recovery		Stoplight	Stat	L
tep 25: To what extent does your security-awareness training program include information and disaster recovery?				
Step 29: Will any mitigation activities change the content of your security awareness trainin contingency planning and disaster recovery? Do you want to make any additional changes to the content of your security awaren			rmatio	on about
Staff Awareness	Ste	p 25	Ste	p 29
The organization's security-awareness training program includes information about the organization's contingency, disaster recovery, and business continuity plans. This training is provided for all employeestime(s) every years.		Current	0	Change
The organization's security-awareness training program includes information about the organization's contingency, disaster recovery, and business continuity plans. This training is provided for new staff members as part of their orientation activities.	0	Current	0	Chang
The organization's security-awareness training program does not include information about the organization's contingency, disaster recovery, and business continuity plans. Staff members learn about contingency, disaster recovery, and		Current		Chang
ousiness continuity plans on their own.				
ousiness continuity plans on their own.	0	Current	<u> </u>	Chang
Step 25: What additional characteristic of your current approach to contingency planning to want to record? Step 29: Will any mitigation activities change this characteristic? Do you want to make any additional changes to this characteristic?	and d		very (
Step 25: What additional characteristic of your current approach to contingency planning to want to record? Step 29: Will any mitigation activities change this characteristic? Do you want to make any additional changes to this characteristic?	and d	isaster reco	very o	do you ep 29
Step 25: What additional characteristic of your current approach to contingency planning to want to record? Step 20: Will any mitigation activities change this characteristic?	and d	isaster reco	St	do you

Protection Strategy Worksheet

7.	Physical	Access	Control
----	-----------------	--------	---------

Stoplight Status

Step 25: Who is currently responsible for physical access control?

Step 29: Will any mitigation activities change responsibility for physical access control?

Do you want to make any additional changes affecting responsibility for physical access control?

Responsibility	Step	25		Step	29	
		Curre	nt		Chang	e
Task	Internal	External	Combined	Internal	External	Combined
Controlling physical access to the building and premises (e.g., controlling visitor access)				a	0	0
Controlling physical access to work areas (e.g., controlling staff and visitor access)	0	0	0	0	0	
Controlling physical access to IT hardware			۵	۵		0
Controlling physical access to software media	0			۵	0	0
	o	0		۵		0
	0		0	<u> </u>	0	
			0	0	۵	0
	0			0		0
	0	0	Ö	0	0	0
	0	0	۵	0		

7. Physical Access Control

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area?

Do you want to make any additional changes to how procedures are documented for this area?

Procedures		Ste	p 25	Ste	р 29
If staff from your organization is partly or completely response	onsible for this area:	*******			
The organization has formally documented plans and procontrolling physical access to the building and premises, hardware, and software media.		<u> </u>	Current		Change
The organization has some formally documented policies controlling physical access to the building and premises, hardware, and software media. Some policies and procedinformal and undocumented.	work areas, IT	-	Current	-	Change
The organization has informal and undocumented plans a controlling physical access to the building and premises, hardware, and software media.		0	Current		Change
		0	Current	۵	Change

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area?

Do you want to make any additional changes to the requirement for attending training in this area?

Training		Ste	ep 25	Ste	р 29
If staff from your organization is partly or completely response	onsible for this area:				
Designated staff members are required to attend training review of the organization's plans and procedures for physical designation.	that includes a vsical access control.		Current		Change
Designated staff members can attend training that include organization's plans and procedures for physical access of it.			Current		Change
The organization generally does not provide opportunitie members to attend training that includes a review of the and procedures for physical access control. Designated stabout physical access control on their own.	organization's plans		Current		Change
			Current		Change

7. Physical Access Control		Stoplight	Stat	us
Third Party A:				
Step 25: To what extent does your organization formally communicate its requirements in t	his ar	ea to this th	ird pa	rty?
Step 29: Will any mitigation activities change how your organization communicates its req	uireme	ents to this t	hird p	arty?
Do you want to make any additional changes to how you communicate requirement	ts to t	his third par	rty?	
Collaborative Issues	Ste	p 25	Ste	р 29
If staff from a third party is partly or completely responsible for this area:				
The organization's requirements for physical access control are formally communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	۵	Current		Change
The organization's requirements for physical access control are informally communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.		Current		Change
The organization's requirements for physical access control are not communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.		Current		Change
		Current		Change
Step 25: To what extent does your organization verify that this third party is addressing re Step 29: Will any mitigation activities change how you verify that this third party is addressing to you want to make any additional changes to how you verify that requirements Verification	ssing r are be	requirement	s in th	? iis area? ep 29
If staff from a third party is partly or completely responsible for this area:	·····			
The organization formally verifies that contractors and service providers have met the requirements for physical access control.	0	Current	۵	Change
The organization informally verifies that contractors and service providers have met the requirements for physical access control.		Current	0	Change
The organization does not verify that contractors and service providers have met the requirements for physical access control.	۵	Current	0	Change
		Current		Change

7. I	Physical	Access	Control
------	----------	--------	----------------

		J		
Third Party B:				
Step 25: To what extent does your organization formally communicate its requirements in t	his ar	ea to this th	ird pa	irty?
Step 29: Will any mitigation activities change how your organization communicates its requirement Do you want to make any additional changes to how you communicate requirement	uirem ts to t	ents to this t his third pa	third p rty?	party?
Collaborative Issues	Ste	ep 25	Ste	p 29
If staff from a third party is partly or completely responsible for this area:				
The organization's requirements for physical access control are formally communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	0	Current	0	Change
The organization's requirements for physical access control are informally communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	0	Current	Q	Change
The organization's requirements for physical access control are not communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.		Current		Change
		Current		Change
Step 25: To what extent does your organization verify that this third party is addressing re-	quirer	nents in this	area	?
Step 29: Will any mitigation activities change how you verify that this third party is addres Do you want to make any additional changes to how you verify that requirements	sing r	equirement		
Verification		ep 25	St	ep 29
If staff from a third party is partly or completely responsible for this area:				
The organization formally verifies that contractors and service providers have met the requirements for physical access control.	0	Current	۵	Change
The organization informally verifies that contractors and service providers have met the requirements for physical access control.	٥	Current	a	Change
The organization does not verify that contractors and service providers have met the requirements for physical access control.	۵	Current	0	Change

☐ Change

☐ Current

8.	Monitoring	and	Auditing	Physical	Security
----	-------------------	-----	----------	-----------------	----------

Stoplight	Status	

Step 25: Who is currently responsible for monitoring and auditing physical security?

Step 29: Will any mitigation activities change responsibility for monitoring and auditing physical security?

Do you want to make any additional changes affecting responsibility for monitoring and auditing physical security?

Responsibility	Step	25		Step	29	
	۰	☐ Current			Chang	ge ļ
Task	Internal	External	Combined	Internal	External	Combined
Keeping maintenance records to document repairs and modifications to IT hardware	0	0	0	٥		0
Monitoring physical access to controlled IT hardware	٥		0	٥		
Monitoring physical access to controlled IT software media	0	0	a	0	0	٥
Monitoring physical access to restricted work areas	0	0		٥	0	
Reviewing monitoring records on a periodic basis		0	0	0	0	
Investigating and addressing any unusual activity that is identified	a	٥	۵	0	0	
	۵			0	0	0
	۵			۵		
	0		0	0	0	0
	0		0	0	0	

8. Monitoring and Auditing Physical Security

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area?

Do you want to make any additional changes to how procedures are documented for this area?

Procedures		Step 25		Step 25		Step 25		Ste	р 29
If staff from your organization is partly or completely resp	onsible for this area:								
The organization has formally documented plans and promonitoring physical access to the building and premises, hardware, and software media.	ocedures for work areas, IT		Current		Change				
The organization has some formally documented policie monitoring physical access to the building and premises hardware, and software media. Some policies and procedinformal and undocumented.	work areas, IT		Current		Change				
The organization has informal and undocumented plans monitoring physical access to the building and premises hardware, and software media.	and procedures for work areas, IT	u	Current		Change				
			Current		Change				

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area?

Do you want to make any additional changes to the requirement for attending training in this area?

Training		Step 25		Step 25		Step 25		Step 25		Step 25		Step 25		Ste	р 29
If staff from your organization is partly or completely response	onsible for this area:														
Designated staff members are required to attend training physical access to the building and premises, work areas, software media.	for monitoring IT hardware, and	٥	Current		Change										
Designated staff members can attend training for monitor to the building and premises, work areas, IT hardware, are they request it.	ring physical access ad software media if		Current		Change										
The organization generally does not provide opportunitie members to attend training for monitoring physical access premises, work areas, IT hardware, and software media. I members learn about monitoring physical access on their	s to the building and Designated staff		Current		Change										
		۵	Current		Change										

8. Monitoring and Auditing Physical Security		Stoplight	Stati	us
Third Party A:				
Step 25: To what extent does your organization formally communicate its requirements in the	is are	ea to this the	rd pa	rty?
Step 29: Will any mitigation activities change how your organization communicates its requirement Do you want to make any additional changes to how you communicate requirement	ireme s to ti	ents to this t his third par	hird p ty?	earty?
Collaborative Issues	Ste	р 25	Ste	p 29
If staff from a third party is partly or completely responsible for this area:				
The organization's requirements for monitoring physical security are formally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.		Current	0	Change
The organization's requirements for monitoring physical security are informally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	0	Current		Change
The organization's requirements for monitoring physical security are not communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	0	Current		Change
		Current	. 🗖	Change
Step 25: To what extent does your organization verify that this third party is addressing rec Step 29: Will any mitigation activities change how you verify that this third party is addres Do you want to make any additional changes to how you verify that requirements to Verification	sing r are be	equirement.	s in th	? is area? ep 29
If staff from a third party is partly or completely responsible for this area:				
The organization formally verifies that contractors and service providers have met the requirements for monitoring physical security.	Q	Current	0	Change
The organization informally verifies that contractors and service providers have met the requirements for monitoring physical security.	0	Current		Change
The organization does not verify that contractors and service providers have met the requirements for monitoring physical security.		Current	<u> </u>	Change
	Q	Current	0	Change

8. Monitoring and Auditing Physical Security

· · · · · · · · · · · · · · · · · · ·		- dia el		9
Step 25: To what extent does your organization formally communicate its requirements in t Step 29: Will any mitigation activities change how your organization communicates its req				
Step 29: Will any mitigation activities change how your organization communicates its req Do you want to make any additional changes to how you communicate requiremen	ts to t	this third pa	rty?	uriy.
Collaborative Issues	Ste	ep 25	Ste	p 29
f staff from a third party is partly or completely responsible for this area:				
The organization's requirements for monitoring physical security are formally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	0	Current	٥	Change
The organization's requirements for monitoring physical security are informally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.		Current		Change
The organization's requirements for monitoring physical security are not communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.		Current		Chang
		Current		Chang
Step 25: To what extent does your organization verify that this third party is addressing re				
Step 29: Will any mitigation activities change how you verify that this third party is addres	quirer	ments in this	s area	?
•	quirer ssing 1 are be	ments in this	s area	
Step 29: Will any mitigation activities change how you verify that this third party is address Do you want to make any additional changes to how you verify that requirements	quirer ssing 1 are be	ments in this requirement eing met?	s area	? nis area?
Step 29: Will any mitigation activities change how you verify that this third party is address Do you want to make any additional changes to how you verify that requirements Verification	quirer ssing 1 are be	ments in this requirement eing met?	s area	? nis area?
Step 29: Will any mitigation activities change how you verify that this third party is address Do you want to make any additional changes to how you verify that requirements Verification If staff from a third party is partly or completely responsible for this area: The organization formally verifies that contractors and service providers have	quirer ssing 1 are be	ments in this requirement eing met?	s area	? iis area? ep 29
Step 29: Will any mitigation activities change how you verify that this third party is address Do you want to make any additional changes to how you verify that requirements Verification If staff from a third party is partly or completely responsible for this area: The organization formally verifies that contractors and service providers have met the requirements for monitoring physical security. The organization informally verifies that contractors and service providers	quirer esing r are be	ments in this requirement eing met? cp 25 Current	s area	? nis area? ep 29 Chang

9.	System	and	Network	Management
----	---------------	-----	---------	------------

Stoplight Status	
------------------	--

Step 25: Who is currently responsible for system and network management?

Step 29: Will any mitigation activities change responsibility for system and network management?

Do you want to make any additional changes affecting responsibility for system and network management?

Responsibility	Step	25		Step	29	
		Curre	nt		Chang	ge
The la	Internal	External	Combined	Internal	External	Combined
Task Configuring IT hardware and software	0	<u> </u>		0	0	
Securely storing sensitive information (e.g., backups stored off site, process for discarding sensitive information)	0		۵	0	0	0
Checking the integrity of installed software	۵			۵	0	
Keeping systems up to date with respect to revisions, patches, and recommendations in security advisories	0	0	0	٥		0
Making and tracking changes to IT hardware and software	٥	۵	0			
Managing passwords, accounts, and privileges	۵	0		٥	٥	a
Selecting system and network management tools	0	۵		0		
	ū	0	ο.	۵	0	
·	a		0	0	0	0
	٥	0	۵	0	0	

9. System and Network Management

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area?

Do you want to make any additional changes to how procedures are documented for this area?

Procedures	Ste	ep 25	Sto	ep 29
If staff from your organization is partly or completely responsible for this ar	ea:			
The organization has formally documented system and network management procedures.	ent 🔲	Current		Change
The organization has some formally documented system and network management procedures. Some procedures in this area are informal and undocumented.		Current		Change
The organization has informal and undocumented system and network management procedures.	0	Current		Change
	_ 0	Current	0	Change

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area?

Do you want to make any additional changes to the requirement for attending training in this area?

Craining		Step 25		Sto	ep 29
f staff from your organization is partly or completely res	ponsible for this area:				
Information technology staff members are required to a managing systems and networks and using system and tools.	attend training for network management		Current	<u>.</u>	Change
Information technology staff members can attend trains systems and networks and using system and network nuthey request it.	ing for managing nanagement tools if	0	Current	0	Change
The organization generally does not provide opportuni technology staff members to attend training for manag networks and using system and network management technology staff members learn about system and network their own.	ing systems and cools. Information	o .	Current		Change
		۵	Current		Change

9. System and Network Management		Stoplight	Dun	
Third Party A:		•		
Step 25: To what extent does your organization formally communicate its requirements in the Step 29: Will any mitigation activities change how your organization communicates its requirement. Do you want to make any additional changes to how you communicate requirement.	iireme	ents to this t	hird p	
Collaborative Issues	Ste	p 25	Ste	р 29
If staff from a third party is partly or completely responsible for this area:				
The organization's security-related system and network management requirements are formally communicated to all contractors and service providers that maintain systems and networks.		Current		Change
The organization's security-related system and network management requirements are informally communicated to all contractors and service providers that maintain systems and networks.	0	Current		Change
The organization's security-related system and network management requirements are not communicated to all contractors and service providers that maintain systems and networks.		Current	0	Change
		C	П	Changa
		Current	Ш	Change
		Current		Change
Step 25: To what extent does your organization verify that this third party is addressing red. Step 29: Will any mitigation activities change how you verify that this third party is address. Do you want to make any additional changes to how you verify that requirements to	quiren sing r are be	nents in this equirement: ing met?	area	? is area?
Step 29: Will any mitigation activities change how you verify that this third party is address. Do you want to make any additional changes to how you verify that requirements of Verification	quiren sing r are be	nents in this	area	?
Step 29: Will any mitigation activities change how you verify that this third party is address. Do you want to make any additional changes to how you verify that requirements to	quiren sing r are be	nents in this equirement: ing met?	area	? is area?
Step 29: Will any mitigation activities change how you verify that this third party is address. Do you want to make any additional changes to how you verify that requirements of the staff from a third party is partly or completely responsible for this area: The organization formally verifies that contractors and service providers have	quiren sing r are be	nents in this equirement: ing met? ep 25	area	? is area? :p 29
Step 29: Will any mitigation activities change how you verify that this third party is address. Do you want to make any additional changes to how you verify that requirements of the staff from a third party is partly or completely responsible for this area: The organization formally verifies that contractors and service providers have met the requirements for security-related system and network management. The organization informally verifies that contractors and service providers have met the requirements for security-related system and network	quirent sing rare be	nents in this equirements ing met? ep 25 Current	area:	is area? Ep 29 Change
Step 29: Will any mitigation activities change how you verify that this third party is address. Do you want to make any additional changes to how you verify that requirements of the contraction. If staff from a third party is partly or completely responsible for this area: The organization formally verifies that contractors and service providers have met the requirements for security-related system and network management. The organization informally verifies that contractors and service providers have met the requirements for security-related system and network management. The organization does not verify that contractors and service providers have	Sto	nents in this equirements ing met? Ep 25 Current Current	area:	cp 29 Change Change

9. System and Network Management

Third Party B:				
Step 25: To what extent does your organization formally communicate its requirements in the				
Step 29: Will any mitigation activities change how your organization communicates its requirement Do you want to make any additional changes to how you communicate requirement	rem s to t	ents to this i his third pa	nıra p rty?	oarty?
Collaborative Issues	Step 25		Ste	р 29
If staff from a third party is partly or completely responsible for this area:				
The organization's security-related system and network management requirements are formally communicated to all contractors and service providers that maintain systems and networks.	0	Current	0	Change
The organization's security-related system and network management requirements are informally communicated to all contractors and service providers that maintain systems and networks.	0	Current	۵	Change
The organization's security-related system and network management requirements are not communicated to all contractors and service providers that maintain systems and networks.		Current	0	Change
		Current		Change
Step 25: To what extent does your organization verify that this third party is addressing requestion Step 29: Will any mitigation activities change how you verify that this third party is address. Do you want to make any additional changes to how you verify that requirements of Verification	sing r are be	requirement	s in th	
If staff from a third party is partly or completely responsible for this area:				
The organization formally verifies that contractors and service providers have met the requirements for security-related system and network management.		Current		Change
The organization informally verifies that contractors and service providers have met the requirements for security-related system and network management.	0	Current	0	Change
The organization does not verify that contractors and service providers have met the requirements for security-related system and network management.		Current	۵	Change

☐ Current ☐ Change

10.	Monitoring	and	Auditing	IT	Securi	ity
-----	------------	-----	----------	----	--------	-----

Stoplight Status	
------------------	--

Step 25: Who is currently responsible for monitoring and auditing IT security?

Step 29: Will any mitigation activities change responsibility for monitoring and auditing IT security?

Do you want to make any additional changes affecting responsibility for monitoring and auditing IT security?

Responsibility	Ster	25		Step	29	
		Curre	nt	.	Chang	;e
Task	Internal	External	Combined	Internal	External	Combined
Using system and network monitoring tools to track system and network activity	٥		٥	0		0
Auditing the firewall and other security components periodically for compliance with policy	0	0	0	0		0
Investigating and addressing any unusual activity that is identified				o o	0	۵
	u	۵	0	0	0	
	0		0	۵		
	o	0	0		Ġ	0
	0			0	۵	۵
	0	0		0		
	0			0	0	٥
	a	0				0

10. Monitoring and Auditing IT Security

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area?

Do you want to make any additional changes to how procedures are documented for this area?

Procedures	Ste	ер 25	Ste	р 29
If staff from your organization is partly or completely responsible	for this area:			
The organization has formally documented procedures for monit network-based access to systems and networks.	oring	Current		Change
The organization has some formally documented procedures for network-based access to systems and networks. Some procedure are informal and undocumented.	monitoring s in this area	Current	Q	Change
The organization has informal and undocumented procedures for network-based access to systems and networks.	r monitoring 🔲	Current		Change
		Current	0	Change

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area?

Do you want to make any additional changes to the requirement for attending training in this area?

Do you want to make any additional enanges to the require					
Training		Ste	ep 25	Ste	р 29
If staff from your organization is partly or completely resp	onsible for this area:				
Information technology staff members are required to att monitoring network-based access to systems and network monitoring and auditing tools.	end training for ks and using		Current	0	Change
Information technology staff members can attend trainin network-based access to systems and networks and using auditing tools if they request it.	g for monitoring monitoring and	Q	Current		Change
The organization generally does not provide opportunition technology staff members to attend training for monitoring access to systems and networks and using monitoring an Information technology staff members learn about monitoring the networks on their own.	ng network-based d auditing tools.		Current		Change
		0	Current	0	Change

10. Monitoring and Auditing IT Security		Stoplight	Stati	us
Third Party A:				
Step 25: To what extent does your organization formally communicate its requirements in the	his are	ea to this thi	rd pa	rty?
Step 29: Will any mitigation activities change how your organization communicates its requirement Do you want to make any additional changes to how you communicate requirement	15 10 11	nis inira par	iy.	
Collaborative Issues	Ste	p 25	Ste	р 29
If staff from a third party is partly or completely responsible for this area:		· · · · · · · · · · · · · · · · · · ·		
The organization's requirements for monitoring information technology security are formally communicated to all contractors and service providers that monitor systems and networks.	0	Current		Change
The organization's requirements for monitoring information technology security are informally communicated to all contractors and service providers that monitor systems and networks.	0	Current	0	Change
The organization's requirements for monitoring information technology security are not communicated to all contractors and service providers that monitor systems and networks.		Current		Change
		Current		Change
Step 25: To what extent does your organization verify that this third party is addressing red. Step 29: Will any mitigation activities change how you verify that this third party is address. Do you want to make any additional changes to how you verify that requirements to	sing r are be	equirements	s in th	? is area? ep 29
Verification				
If staff from a third party is partly or completely responsible for this area: The organization formally verifies that contractors and service providers have met the requirements for monitoring information technology security.	D	Current	0	Change
The organization informally verifies that contractors and service providers have met the requirements for monitoring information technology security.	<u> </u>	Current	0	Change
The organization does not verify that contractors and service providers have met the requirements for monitoring information technology security.	۵	Current	0	Change
	0	Current		Change

10. Monitoring and Auditing IT Security

Chird Party B:			_	_
Step 25: To what extent does your organization formally communicate its requirements in t				
Step 29: Will any mitigation activities change how your organization communicates its requiremen Do you want to make any additional changes to how you communicate requiremen	iireme ts to tl	ents to this this this third par	rty?	
Collaborative Issues	Ste	p 25	Ste	р 29
If staff from a third party is partly or completely responsible for this area:			,,,	
The organization's requirements for monitoring information technology security are formally communicated to all contractors and service providers that monitor systems and networks.		Current	0	Change
The organization's requirements for monitoring information technology security are informally communicated to all contractors and service providers that monitor systems and networks.	0	Current		Change
The organization's requirements for monitoring information technology security are not communicated to all contractors and service providers that		Current		Change
monitor systems and networks.				
	0	Current		Change
	quiren	nents in this		?
monitor systems and networks. Step 25: To what extent does your organization verify that this third party is addressing respectively. Step 29: Will any mitigation activities change how you verify that this third party is addressing respectively.	quirentsing rare be	nents in this	s in th	?
monitor systems and networks. Step 25: To what extent does your organization verify that this third party is addressing re Step 29: Will any mitigation activities change how you verify that this third party is address Do you want to make any additional changes to how you verify that requirements	quirentsing rare be	nents in this equirement: ing met?	s in th	? is area?
monitor systems and networks. Step 25: To what extent does your organization verify that this third party is addressing restep 29: Will any mitigation activities change how you verify that this third party is address Do you want to make any additional changes to how you verify that requirements Verification	quiren sing r are be	nents in this equirement: ing met?	s in th	? is area?
Step 25: To what extent does your organization verify that this third party is addressing restep 29: Will any mitigation activities change how you verify that this third party is address Do you want to make any additional changes to how you verify that requirements Verification If staff from a third party is partly or completely responsible for this area: The organization formally verifies that contractors and service providers have	quiren sing r are be	nents in this requirement: ring met?	s in th	? is area? ep 29
Step 25: To what extent does your organization verify that this third party is addressing re Step 29: Will any mitigation activities change how you verify that this third party is address Do you want to make any additional changes to how you verify that requirements Verification If staff from a third party is partly or completely responsible for this area: The organization formally verifies that contractors and service providers have met the requirements for monitoring information technology security. The organization informally verifies that contractors and service providers	quirent sing rare be	nents in this requirement. ring met? rep 25 Current	Sto	? is area? ep 29 Change
Step 25: To what extent does your organization verify that this third party is addressing re Step 29: Will any mitigation activities change how you verify that this third party is address Do you want to make any additional changes to how you verify that requirements Verification If staff from a third party is partly or completely responsible for this area: The organization formally verifies that contractors and service providers have met the requirements for monitoring information technology security. The organization informally verifies that contractors and service providers have met the requirements for monitoring information technology security. The organization does not verify that contractors and service providers have	quirent sing rare be	nents in this requirements ring met? cp 25 Current Current	Sto	? is area? ep 29 Change

11.	Antl	hentica	tion	and	Auth	ioriza	tion
-----	------	---------	------	-----	------	--------	------

Stoplight	Status	
Stopingin	Status	

Step 25: Who is currently responsible for authentication and authorization?

Step 29: Will any mitigation activities change responsibility for authentication and authorization?

Do you want to make any additional changes affecting responsibility for authentication and authorization?

Responsibility	Step	25		Step	29	
		Curre	nt	ם	Chang	e,
Task	Internal	External	Combined	Internal	External	Combined
Implementing access controls (e.g., file permissions, network configuration) to restrict user access to information, sensitive systems, specific applications and services, and network connections	٥			a	0	0
Implementing user authentication (e.g., passwords, biometrics) to restrict user access to information, sensitive systems, specific applications and services, and network connections		0		0	0	0
Establishing and terminating access to systems and information for both individuals and groups	0	0	0	٥		0
	۵	0	Q			۵
	0	0	Q			D
	0	۵	0	0		0
,	0	o		0		0
		0		u	٥	
	0	0	0		0	Q
	a	۵	0	٥	0	0

11. Authentication and Authorization

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area?

Do you want to make any additional changes to how procedures are documented for this area?

Procedures	St	tep 25	Ste	р 29
If staff from your organization is partly or completely resp	onsible for this area:			
The organization has formally documented authorization procedures for restricting user access to information, ser specific applications and services, and network connecti	sitive systems,	Current	0	Change
The organization has some formally documented author authentication procedures for restricting user access to it systems, specific applications and services, and network procedures in this area are informal and undocumented.	nformation, sensitive	Current		Change
The organization has informal and undocumented autho authentication procedures for restricting user access to it systems, specific applications and services, and network	nformation, sensitive	Current		Change
		Current		Change

Step 25: To what extent are staff members required to attend training in this area?

Training		Sto	ep 25	Ste	р 29
If staff from your organization is partly or completely resp	onsible for this area:			,,	
Information technology staff members are required to at implementing technological measures to restrict user acc sensitive systems, specific applications and services, and connections.	ess to information,	. 🗅	Current		Change
Information technology staff members can attend training technological measures to restrict user access to informations systems, specific applications and services, and network request it.	tion, sensitive	0	Current		Change
The organization generally does not provide opportuniti technology staff members to attend training for implementation measures to restrict user access to information, sensitive applications and services, and network connections. Information and authorization and authorization and authorization.	enting technological systems, specific formation technology		Current	0	Change
			Current	0	Change

A A A A A A A A A A A A A A A A A A A		Stoplight	Stati	us			
11. Authentication and Authorization		pg					
Third Party A:							
Step 25: To what extent does your organization formally communicate its requirements in the	iis ar	ea to this th	ird pa	rty?			
Step 29: Will any mitigation activities change how your organization communicates its requirement Do you want to make any additional changes to how you communicate requirement	irem s to t	ents to this t his third pa	hird p rty?	party?			
Collaborative Issues	Ste	ep 25	Ste	р 29			
If staff from a third party is partly or completely responsible for this area:							
The organization's requirements for controlling access to systems and information are formally communicated to all contractors and service providers that provide authentication and authorization services.		Current		Change			
The organization's requirements for controlling access to systems and information are informally communicated to all contractors and service providers that monitor systems and networks.	0	Current	0	Change			
The organization's requirements for controlling access to systems and information are not communicated to all contractors and service providers that monitor systems and networks.		Current		Change			
		Current		Change			
Step 25: To what extent does your organization verify that this third party is addressing requirements in this area? Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met? Verification Step 25 Step 29							
If staff from a third party is partly or completely responsible for this area:			•				
The organization formally verifies that contractors and service providers have met the requirements for authentication and authorization.	0	Current	۵	Change			
The organization informally verifies that contractors and service providers have met the requirements for authentication and authorization.	0	Current	Q	Change			
The organization does not verify that contractors and service providers have met the requirements for authentication and authorization.	0	Current	٥	Change			
	_			Change			

11. Authentication and Authorization

Do you want to make any additional changes to how you communicate requiremen Collaborative Issues		p 25		р 29
If staff from a third party is partly or completely responsible for this area:				
The organization's requirements for controlling access to systems and information are formally communicated to all contractors and service providers that provide authentication and authorization services.	٥	Current		Change
The organization's requirements for controlling access to systems and information are informally communicated to all contractors and service providers that monitor systems and networks.	٥	Current	0	Change
The organization's requirements for controlling access to systems and information are not communicated to all contractors and service providers that monitor systems and networks.	0	Current	0	Change
		Current		Change
Step 25: To what extent does your organization verify that this third party is addressing re				
Step 20. Will any mitigation activities change how you verify that this third party is addres	ssing r	requirement		
	ssing r are be	requirement	s in th	
Step 29: Will any mitigation activities change how you verify that this third party is addres Do you want to make any additional changes to how you verify that requirements	ssing r are be	requirement eing met?	s in th	is area?
Step 29: Will any mitigation activities change how you verify that this third party is addres Do you want to make any additional changes to how you verify that requirements Verification	ssing r are be	requirement eing met?	s in th	is area?
Step 29: Will any mitigation activities change how you verify that this third party is address Do you want to make any additional changes to how you verify that requirements Verification If staff from a third party is partly or completely responsible for this area: The organization formally verifies that contractors and service providers have	ssing r are be	requirement eing met? ep 25	Sto	ep 29
Step 29: Will any mitigation activities change how you verify that this third party is address Do you want to make any additional changes to how you verify that requirements Verification If staff from a third party is partly or completely responsible for this area: The organization formally verifies that contractors and service providers have met the requirements for authentication and authorization. The organization informally verifies that contractors and service providers	ssing r are be St	requirement eing met? ep 25	Sto	ep 29 Chang

12.	Vul	lnerability	Management	t
-----	-----	-------------	------------	---

Stoplight	Status	

Step 25: Who is currently responsible for vulnerability management?

Step 29: Will any mitigation activities change responsibility for vulnerability management?

Do you want to make any additional changes affecting responsibility for vulnerability management?

Responsibility	St	ep 25		Step	29	
		Curre	nt	۰	Chang	ge l
Tools.	Internal	External	Combined	Internal	External	Combined
Task Selecting vulnerability evaluation tools, checklists, and scripts	0	0	۵	0		0
Scheduling and performing technology vulnerability evaluations on a periodic basis	0	0	٥	٥	0	
Keeping up to date with known vulnerability types and attack methods			۵	٥	0	0
Reviewing sources of information on vulnerability announcements, securi alerts, and notices	ty			0		۵
Interpreting the results of technology vulnerability evaluations	0			٥	0	0
Addressing technology vulnerabilities that are identified		۵		0		o l
Maintaining secure storage and disposition of technology vulnerability da	ta 🗖		0	٥	0	۵
	_ 0					a
	_ 0	Q	٥	o	D	0
		D	0			Q

12. Vulnerability Management

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area?

Do you want to make any additional changes to how procedures are documented for this area?

Procedures		Ste	p 25	Ste	p 29
If staff from your organization is partly or completely respo	onsible for this area:				
The organization has formally documented vulnerability management procedures.		a	Current		Change
The organization has some formally documented vulnerability management procedures. Some procedures in this area are informal and undocumented.		<u> </u>	Current		Change
The organization has informal and undocumented vulner procedures.	ability management (0	Current	۵	Change
		0	Current		Change

Step 25: To what extent are staff members required to attend training in this area?

Training		Ste	ep 25	Ste	р 29
If staff from your organization is partly or completely resp	onsible for this area:				
Information technology staff members are required to attend training for managing technology vulnerabilities and using vulnerability evaluation tools.			Current	0	Change
Information technology staff members can attend training technology vulnerabilities and using vulnerability evaluation request it.	ng for managing ation tools if they		Current	0	Change
The organization generally does not provide opportunitie technology staff members to attend training for managing vulnerabilities and using vulnerability evaluation tools. technology staff members learn about vulnerability management.	ng technology Information		Current		Change
		0	Current	0	Change

12. Vulnerability Management		Stoplight	Statı	ıs
Third Party A:				
Step 25: To what extent does your organization formally communicate its requirements in the	is are	a to this thi	rd pa	rty?
Step 29: Will any mitigation activities change how your organization communicates its requirements. Do you want to make any additional changes to how you communicate requirements.	ireme s to th	nts to this ti is third par	•,, •	
Collaborative Issues	Ste	p 25	Ste	p 29
If staff from a third party is partly or completely responsible for this area:				
The organization's vulnerability management requirements are formally communicated to all contractors and service providers that manage technology vulnerabilities.	0	Current		Change
The organization's vulnerability management requirements are informally communicated to all contractors and service providers that manage technology vulnerabilities.		Current	0	Change
The organization's vulnerability management requirements are not communicated to all contractors and service providers that manage technology vulnerabilities.	٥	Current	a	Change
		Current	<u> </u>	Change
Step 25: To what extent does your organization verify that this third party is addressing req Step 29: Will any mitigation activities change how you verify that this third party is address	ing re	equirements	area s in th	? is area?
Do you want to make any additional changes to how you verify that requirements a	., с ос	ing mer.		
Verification	Sto	ep 25	St	ep 29
If staff from a third party is partly or completely responsible for this area:		<u> </u>	<u></u>	
The organization formally verifies that contractors and service providers have met the requirements for vulnerability management.		Current	0	Change
The organization informally verifies that contractors and service providers have met the requirements for vulnerability management.	0	Current		Change
The organization does not verify that contractors and service providers have met the requirements for vulnerability management.		Current	0	Change
		Current	0	Change

12. Vulnerability Management

Collaborative Issues		Sto	ep 25	Ste	р 29
If staff from a third party is partly or completely respo	onsible for this area:		,	ne contrate and 100 mm	
The organization's vulnerability management requi communicated to all contractors and service provide technology vulnerabilities.	rements are formally ers that manage		Current	0	Change
The organization's vulnerability management requi communicated to all contractors and service provide technology vulnerabilities.	rements are informally ers that manage		Current	0	Change
The organization's vulnerability management requi communicated to all contractors and service provid technology vulnerabilities.	rements are not ers that manage	0	Current		Change
			Current	0	Change

Si	Step 25		р 29
ve 🔲	Current		Change
۵	Current	0	Change
	Current		Change
_ 🗆	Current		Change
		Current Current Current	Current Curren

Stoplight Status	
------------------	--

Step 25: Who is currently responsible for encryption?

Step 29: Will any mitigation activities change responsibility for encryption?

Do you want to make any additional changes affecting responsibility for encryption?

Responsibility	Step	25		Step	29	
	<u> </u>	Curre	ent			ge
Task	Internal	External	Combined	Internal	External	Combined
Implementing encryption technologies to protect sensitive information that is electronically stored and transmitted (e.g., data encryption, public key infrastructure, virtual private network technology)	0	۵	0	0	0	0
Implementing encrypted protocols for remotely managing systems, routers, and firewalls	a	0		o ·	0	0
and moveme				0	۵	0
	0	0		۵	0	0
	0				۵	0
	۵		۵	۵	0	0
	a	٥	0	a	0	

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area?

Do you want to make any additional changes to how procedures are documented for this area?

Procedures		Ste	ep 25	Ste	р 29
If staff from your organization is partly or completely response	onsible for this area:				
The organization has formally documented procedures for using encryption technologies.		۵	Current	0	Change
The organization has some formally documented procedimplementing and using encryption technologies. Some parea are informal and undocumented.	ures for procedures in this	a	Current	۵	Change
The organization has informal and undocumented proced implementing and using encryption technologies.	lures for	۵	Current	۵	Change
Imponenting and and and		a	Current	0	Change
		<u> </u>		<u> </u>	

13. Encryption

Step 25: To what extent are IT staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area?

Do you want to make any additional changes to the requirement for attending training in this area?

Information Technology Staff Training	·	Step	25	Ste	р 29
If staff from your organization is partly or completely respon	nsible for this area:				
Information technology staff members are required to atte implementing encryption technologies.	nd training for [Current	0	Change
Information technology staff members can attend training encryption technologies if they request it.	for implementing [Current		Change
The organization generally does not provide opportunities technology staff members to attend training for implement technologies. Information technology staff members learn implementing encryption technologies on their own.	ting encryption	a (Current		Change
		0 (Current		Change

Step 25: To what extent are staff members required to attend training in this area?

Staff Training	Ste	ep 25	Sto	ep 29
All staff members are required to attend training for using encryption technologies.		Current		Current
All staff members can attend training for using encryption technologies if they request it.		Current	۵	Current
The organization generally does not provide opportunities for staff members to attend training for using encryption technologies. Staff members learn about using encryption technologies on their own.		Current		Change
		Current	0	Change

13. Encryption		Stoplight	Stati	us
Third Party A:				
Step 25: To what extent does your organization formally communicate its requirements in the				
Step 29: Will any mitigation activities change how your organization communicates its requirement Do you want to make any additional changes to how you communicate requirement	iireme ts to ti	ents to this t his third par	riy:	
Collaborative Issues	Ste	ep 25	Ste	p 29
If staff from a third party is partly or completely responsible for this area:	.,			
The organization's requirements for protecting sensitive information are formally communicated to all contractors and service providers that provide encryption technologies.		Current	0	Change
The organization's requirements for protecting sensitive information are informally communicated to all contractors and service providers that provide encryption technologies.	0	Current		Change
The organization's requirements for protecting sensitive information are not communicated to all contractors and service providers that provide encryption technologies.	٥	Current	۵	Change
		Current		Change
Step 25: To what extent does your organization verify that this third party is addressing req Step 29: Will any mitigation activities change how you verify that this third party is address Do you want to make any additional changes to how you verify that requirements of	sing r are be	requirements ring met?	s in th	is area?
Verification	Sto	ep 25	Sto	ep 29
If staff from a third party is partly or completely responsible for this area:				
The organization formally verifies that contractors and service providers have met the requirements for implementing encryption technologies.		Current	<u> </u>	Change
The organization informally verifies that contractors and service providers have met the requirements for implementing encryption technologies.	<u> </u>	Current	0	Change
The organization does not verify that contractors and service providers have met the requirements for implementing encryption technologies.	0	Current	<u> </u>	Change
	0	Current		Change

13.]	Encryp	tion
--------------	--------	------

		10		J Pulon
Third Party B:				
Step 25: To what extent does your organization formally communicate its requirements in the				
Step 29: Will any mitigation activities change how your organization communicates its requ Do you want to make any additional changes to how you communicate requirement	irem ts to t	ents to this his third pa	third p rty?	party?
Collaborative Issues	Step 25 Step 29			ер 29
If staff from a third party is partly or completely responsible for this area:			***********************	
The organization's requirements for protecting sensitive information are formally communicated to all contractors and service providers that provide encryption technologies.	٥	Current		Change
The organization's requirements for protecting sensitive information are informally communicated to all contractors and service providers that provide encryption technologies.	0	Current	0	Change
The organization's requirements for protecting sensitive information are not communicated to all contractors and service providers that provide encryption technologies.	0	Current	٥	Change
	٥	Current		Change
Step 25: To what extent does your organization verify that this third party is addressing req Step 29: Will any mitigation activities change how you verify that this third party is address Do you want to make any additional changes to how you verify that requirements of Verification	sing r are be	equirement	s in th	
If staff from a third party is partly or completely responsible for this area:				
The organization formally verifies that contractors and service providers have met the requirements for implementing encryption technologies.	۵	Current	0	Change
The organization informally verifies that contractors and service providers have met the requirements for implementing encryption technologies.	0	Current	0	Change
The organization does not verify that contractors and service providers have met the requirements for implementing encryption technologies.	0	Current	0	Change

☐ Change

Current

14.	Security	Architecture	and	Design
-----	----------	--------------	-----	--------

Stoplight	Status		
		I	

Step 25: Who is currently responsible for security architecture and design?

Step 29: Will any mitigation activities change responsibility for security architecture and design?

Do you want to make any additional changes affecting responsibility for security architecture and design?

Responsibility	Ste	25		Ste	29	
	۵	Curre	nt	a	Chang	ge
Task	Internal	External	Combined	Internal	External	Combined
Designing security controls in new and revised systems and networks	0		0	٥	0	
Documenting and revising diagrams that show the enterprise-wide security architecture and network topology	۵	0		٥		0
	۵		0	a		۵
	0		۵	0		
	0		0		0	0
	0	0		0		
	0	0	Ö		0	
	o			a		۵
	0	-	0	0	۵	0
				٥		

14. Security Architecture and Design

Step 25: To what extent are practices for this area formally documented?

Step 29: Will any mitigation activities change the extent to which practices are formally documented for this area?

Do you want to make any additional changes to how practices are documented for this area?

Procedures		Ste	ep 25	Sto	ер 29
If staff from your organization is partly or completely resp	onsible for this area:				
The organization has formally documented security arch practices.	itecture and design		Current	0	Change
The organization has some formally documented securit design practices. Some practices in this area are informations of the control of the co	y architecture and l and undocumented.		Current		Change
The organization has informal and undocumented securidesign practices.	ty architecture and		Current	۵	Change
			Current		Change

Step 25: To what extent are staff members required to attend training in this area?

Curr	rent (<u> </u>	Change
Curr	rent	<u> </u>	Change
Curr	rent	٥	Change
☐ Curr	rent	٥	Change
	Curr	Current Current Current Current Current	Current C

14. Security Architecture and Design Stoplight Status			us	
Third Party A:				
Step 25: To what extent does your organization formally communicate its requirements in to Step 29: Will any mitigation activities change how your organization communicates its requirement Do you want to make any additional changes to how you communicate requirement	uirem	ents to this i	third p	
Collaborative Issues	Sto	ep 25	Ste	р 29
If staff from a third party is partly or completely responsible for this area:				
The organization's security-related requirements are formally communicated to all contractors and service providers that design systems and networks.		Current	0	Change
The organization's security-related requirements are informally communicated to all contractors and service providers that design systems and networks.		Current		Change
The organization's security-related requirements are not communicated to all contractors and service providers that design systems and networks.		Current		Change
		Current	0	Change
Step 25: To what extent does your organization verify that this third party is addressing req				
Step 29: Will any mitigation activities change how you verify that this third party is address. Do you want to make any additional changes to how you verify that requirements of	sing r are be	equirements ing met?	s in th	is area?
Verification	Sto	ep 25	Ste	ep 29
If staff from a third party is partly or completely responsible for this area:				
The organization formally verifies that contractors and service providers have met the requirements for security architecture and design.		Current	0	Change
The organization informally verifies that contractors and service providers have met the requirements for security architecture and design.		Current	٥	Change
The organization does not verify that contractors and service providers have met the requirements for security architecture and design.	•	Current	0	Change
	۵	Current	0	Change

14. Security Architecture and Design

Third Party B:				
Step 25: To what extent does your organization formally communicate its requirements in the	nis ar	ea to this th	ird pa	rty?
Step 29: Will any mitigation activities change how your organization communicates its requirement Do you want to make any additional changes to how you communicate requirement	iireme ts to t	ents to this i his third pa	hird prty?	party?
Collaborative Issues	Ste	ep 25	Ste	р 29
If staff from a third party is partly or completely responsible for this area:				
The organization's security-related requirements are formally communicated to all contractors and service providers that design systems and networks.	0	Current	٥	Change
The organization's security-related requirements are informally communicated to all contractors and service providers that design systems and networks.		Current	0	Change
The organization's security-related requirements are not communicated to all contractors and service providers that design systems and networks.		Current	۵	Change
		Current		Change
Step 25: To what extent does your organization verify that this third party is addressing req Step 29: Will any mitigation activities change how you verify that this third party is address. Do you want to make any additional changes to how you verify that requirements of Verification	sing r are be	equirement	s in th	
If staff from a third party is partly or completely responsible for this area:				
The organization formally verifies that contractors and service providers have met the requirements for security architecture and design.	0	Current		Change
The organization informally verifies that contractors and service providers have met the requirements for security architecture and design.		Current		Change
The organization does not verify that contractors and service providers have met the requirements for security architecture and design.		Current	0	Change
		Current		Change

Stoplight	Status	
I B		•

Step 25: Who is currently responsible for incident management?

Step 29: Will any mitigation activities change responsibility for incident management?

Do you want to make any additional changes affecting responsibility for incident management?

Responsibility	Ste	25		Ster	29	
		Curre	nt	a	Chang	e
Task	Internal	External	Combined	Internal	External	Combined
Documenting and revising procedures for identifying, reporting, and responding to suspected security incidents and violations	a	0	0	0	0	۵
Documenting and revising policies and procedures for working with law enforcement agencies	٥		0	0	0	0
Testing incident management procedures on a periodic basis	o			۵	0	
	o o			٥		0
	0	0		۵	0	
	o o	0		0	0	
	۵	0	0	0		0
	0		0	0		
		0	0	٥		0
	0	0		0	0	

15. Incident Management

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area?

Do you want to make any additional changes to how procedures are documented for this area?

Procedures	Step	25	Ste	р 29
If staff from your organization is partly or completely responsible for this area	•			
The organization has formally documented incident management procedures.		Current		Change
The organization has some formally documented incident management procedures. Some procedures in this area are informal and undocumented.		Current		Change
The organization has informal and undocumented incident management procedures.		Current		Change
	u (Current		Change

Step 25: To what extent are staff members required to attend training in this area?

Training		Ste	ep 25	Ste	ер 29
If staff from your organization is partly or completely respo	nsible for this area:				
Designated staff members are required to attend training management.	or incident	a	Current	•	Change
Designated staff members can attend training for incident request it.	management if they	0	Current		Change
The organization generally does not provide opportunities members to attend training for incident management. Des members learn about incident management on their own.	s for designated staff ignated staff		Current		Change
			Current	0	Change

15. Incident Management		Stoplight	Stat	us
Third Party A:				
Step 25: To what extent does your organization formally communicate its requirements in the				
Step 29: Will any mitigation activities change how your organization communicates its requirement. Do you want to make any additional changes to how you communicate requirement.	ireme ts to t	ents to this t his third par	hird p rty?	party?
Collaborative Issues	Ste	ep 25	Ste	ер 29
If staff from a third party is partly or completely responsible for this area:				
The organization's requirements for managing incidents are formally communicated to all contractors and service providers that provide incident management services.	0	Current	<u> </u>	Change
The organization's requirements for managing incidents are informally communicated to all contractors and service providers that provide incident management services.		Current		Change
The organization's requirements for managing incidents are not communicated to all contractors and service providers that provide incident management services.		Current		Change
		Current	<u> </u>	Change
Step 25: To what extent does your organization verify that this third party is addressing req Step 29: Will any mitigation activities change how you verify that this third party is address Do you want to make any additional changes to how you verify that requirements a Verification	sing re are bei	equirements	in th	
If staff from a third party is partly or completely responsible for this area:				
The organization formally verifies that contractors and service providers have met the requirements for managing incidents.		Current	0	Change
The organization informally verifies that contractors and service providers have met the requirements for managing incidents.		Current	0	Change
The organization does not verify that contractors and service providers have met the requirements for managing incidents.	0	Current	0	Change
	•	Current		Change

15.	Incident	Management
-----	----------	------------

				Ü
Third Party B:				
Step 25: To what extent does your organization formally communicate its requirements in t	his ar	rea to this th	ird pa	irty?
Step 29: Will any mitigation activities change how your organization communicates its requirement Do you want to make any additional changes to how you communicate requirement	uirem ts to t	ents to this t his third pa	third p rty?	party?
Collaborative Issues	Ste	ep 25	Ste	р 29
If staff from a third party is partly or completely responsible for this area:				
The organization's requirements for managing incidents are formally communicated to all contractors and service providers that provide incident management services.	0	Current	0	Change
The organization's requirements for managing incidents are informally communicated to all contractors and service providers that provide incident management services.	0	Current	0	Change
The organization's requirements for managing incidents are not communicated to all contractors and service providers that provide incident management services.	0	Current	0	Change
		Current		Change
Step 25: To what extent does your organization verify that this third party is addressing rec Step 29: Will any mitigation activities change how you verify that this third party is addres Do you want to make any additional changes to how you verify that requirements to Verification	sing r are be	requirement	s in th	
If staff from a third party is partly or completely responsible for this area:				
The organization formally verifies that contractors and service providers have met the requirements for managing incidents.	0	Current	۵	Change
The organization informally verifies that contractors and service providers have met the requirements for managing incidents.		Current	٥	Change
The organization does not verify that contractors and service providers have met the requirements for managing incidents.	٥	Current	0	Change
	0	Current		Change

Phase 3
Process S5
Activity S5.3

Mitigation Activities Guide

The *Mitigation Activities Guide* describes potential mitigation activities for each security practice area. You will find examples of mitigation activities related to each security practice area in this guide.

Security Practice Area	Page
1. Security Awareness and Training	84
2. Security Strategy	86
3. Security Management	88
4. Security Policies and Regulations	90
5. Collaborative Security Management	92
6. Contingency Planning/Disaster Recovery	94
7. Physical Access Control	96-97
8. Monitoring and Auditing Physical Security	98-99
9. System and Network Management	100-101
10. Monitoring and Auditing IT Security	102-103
11. Authentication and Authorization	104-105
12. Vulnerability Management	106-107
13. Encryption	108-109
14. Security Architecture and Design	110-111
15. Incident Management	112-113

1. Security Awareness and Training	Candidate Mitigation Activitie	
Mitigation Activity		Protection Strategy Link
Develop and document a training strategy the awareness training and security-related trainitechnologies.	at includes security ing for supported	Training Strategy
Provide periodic security awareness training periodic basis (e.g.,time(s) every	for all employees on a years).	Security Awareness Training
Provide security awareness training for <i>new</i> their orientation activities.	staff members as part of	Security Awareness Training
Require IT staff members to attend security-technologies that they support.	related training for any	Security-Related Training for Supported Technologies
Enable IT staff members to attend security-retechnologies that they support.	elated training for any	Security-Related Training for Supported Technologies
Implement a <i>formal</i> mechanism for providing staff members with periodic updates/bulletins about important security issues.		Periodic Security Updates
Implement an <i>informal</i> mechanism for providing staff members with periodic updates/bulletins about important security issues.		Periodic Security Updates
Implement a <i>formal</i> mechanism for tracking and verifying that staff members receive appropriate security-related training.		Training Verification
Implement an <i>informal</i> mechanism for tracking staff members receive appropriate security-re	ing and verifying that elated training.	Training Verification
Schedule a one-time offering of security awa	Schedule a one-time offering of security awareness training.	
Send selected staff members to training for a a limited or one-time offering in a specific te	specific technology (i.e., echnology).	
Cross train selected staff members to use specific information systems and/or applications. Cross-trained staff members will back up the primary users of those systems and/or applications.		
Cross train selected staff members to provide specific skills or services. Cross-trained staff members will back up the staff members who normally provide those skills or services.		
Cross train selected IT staff members to conspecific information systems, networks, and trained IT staff members will back up the proormally maintain those systems, networks,	or applications. Cross- imary administrators who	
Ensure that selected staff members understar with third parties that own or operate key sy be able to work with third parties when there systems owned and/or operated by those thir	stems. These people will e are problems with	

2. Security Strategy		Candidate Mitigation Activities
Mitigation Activity		Protection Strategy Link
Implement a formal mechanism for integrati security considerations into busines business strategies and goals into se policies	s strategies	Business and Security Strategy Integration
Implement an <i>informal</i> mechanism for integrating • security considerations into business strategies • business strategies and goals into security strategies and policies		Business and Security Strategy Integration
Document security strategies, goals, and objeinformation security.	ectives for all aspects of	Documented Strategies
Document the security strategies, goals, and security-related areas.	objectives for selected	Documented Strategies
Incorporate information about the organization the organization's security-awareness training		Staff Awareness

3. Security Management		Candidate Mitigation Activities
Mitigation Activity		Protection Strategy Link
Document information security roles and resin the organization.	ponsibilities for all staff	Roles and Responsibilities
Document information security roles and res	ponsibilities for selected	Roles and Responsibilities
Include a separate line item for information organization's budget.	security activities in the	Funding
Include a separate line item for information organization's information technology budge	security activities in et.	Funding
Use the results of an information security ris the level of funding for information security	k evaluation to determine activities.	Funding
Document procedures for including security organization's hiring and termination process	considerations in the sees.	Human Resource Procedures
Document a process for assessing and mana information security risks.	iging the organization's	Risk Management
Document a process for assessing the organ security risks.	ization's information	Risk Management
Incorporate information about the organization's management process into the organization's training program.	ion's security security-awareness	Staff Awareness
Implement a formal mechanism for providir summaries of important security-related info	ng managers with ormation.	Management Awareness
Implement an informal mechanism for prov summaries of important security-related info	iding managers with ormation.	Management Awareness

4. Security Policies and Regulations		Candidate Mitigation Activities
Mitigation Activity		Protection Strategy Link
Document a comprehensive set of security-re	elated policies.	Documented Policies
Document security-related policies for select	ted areas.	Documented Policies
Implement a formal mechanism for <i>creating</i> related policies.	and updating security-	Policy Management
Implement a formal mechanism for creating	security-related policies.	Policy Management
Implement formal procedures for enforcing s	security-related policies.	Policy Enforcement
Incorporate information about the organization's security policies and regulations into the organization's security-awareness training program.		Staff Awareness
Document procedures for complying with all information security policies, applicable laws and regulations, and insurance requirements.		Policy and Regulation Compliance
Document procedures for complying with selected security policies, applicable laws and regulations, and insurance requirements.		Policy and Regulation Compliance

5. Collaborative Security Management		Candidate Mitigation Activities
Mitigation Activity		Protection Strategy Link
Document policies and procedures for protect working with collaborators and partners.	ting information when	Collaborators and Partners
Document policies and procedures for protect working with contractors and subcontractors	ting information when	Contractors and Subcontractors
Document policies and procedures for protect working with service providers.	eting information when	Service Providers
Implement a <i>formal</i> mechanism (e.g., contraction communicating information protection requitable) third parties.	ct mechanism) for rements to all appropriate	Requirements
Implement an <i>informal</i> mechanism (e.g., ass communicating information protection requithird parties.	ign responsibility) for rements to all appropriate	Requirements
Implement a <i>formal</i> mechanism (e.g., contract mechanism) for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet the organization's information protection requirements.		Verification
Implement an <i>informal</i> mechanism (e.g., assign responsibility) for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet the organization's information protection requirements.		Verification
Incorporate information about the organizati procedures for collaborative security manage organization's security-awareness training p	ement into the	Staff Awareness

6. Contingency Planning/Disaster Recovery	C	andidate Mitigation Activities
Mitigation Activity	Pro	otection Strategy Link
Perform an analysis defining the criticality of all applications, and data.	operations, Bu	siness Operations Analysis
Perform an analysis defining the criticality of seleapplications, and/or data.	ected operations, Bu	siness Operations Analysis
Document business continuity or emergency oper recovery plan(s), and contingency plan(s) for respense regencies.	acton prairie, and	ocumented Plans
Document a subset of the following plans for respenses emergencies: business continuity or emergency disaster recovery plan(s), and contingency plan(s)	operation plans,	ocumented Plans
Formally test the organization's business continu operation plans, disaster recovery plan(s), and co responding to emergencies.	10, 01 011101 841119	sted Plans
Formally test a subset of the following plans for a emergencies: business continuity or emergency of disaster recovery plan(s), and contingency plan(s)	peration plans,	ested Plans
Incorporate contingency plans into the organization recovery and business continuity plans for access information.	OIL D WILDWOTT	formation Access
Incorporate information about the organization's recovery, and business continuity plans into the esecurity-awareness training program.		aff Awareness
Document a disaster recovery plan for a specific by the information technology staff.	system maintained	
Develop a disaster recovery plan for a specific sy third party.	stem maintained by a	
Document a business continuity plan for specific business processes.		
Purchase insurance for any security problems rel system.	ated to a specific	
Configure and maintain a hot backup for a system	n	
Configure and maintain a cold backup for a spec	ific system.	_

7. Physical Access Control	Candidate Mitigation Activities	
Mitigation Activity		Protection Strategy Link
Change responsibility for controlling physica and premises (e.g., controlling visitor access)	al access to the building).	Responsibility
Change responsibility for controlling physica (e.g., controlling staff and visitor access).	al access to work areas	Responsibility
Change responsibility for controlling physica	al access to IT hardware.	Responsibility
Change responsibility for controlling physica media.	al access to software	Responsibility
Document formal procedures for controlling building and premises, work areas, IT hardw	physical access to the are, and software media.	Procedures
Send selected staff members to training for country to the building and premises, work areas, IT media.	controlling physical access hardware, and software	Training
Implement a <i>formal</i> mechanism (e.g., contra communicating the organization's requirement control to all appropriate contractors, service parties. Assign responsibility for working discontractors, service providers, and third part members.	ents for physical access e providers, and third irectly with those	Collaborative Issues
Implement an <i>informal</i> mechanism (e.g., assign responsibility) for communicating the organization's requirements for physical access control to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Collaborative Issues
Implement a <i>formal</i> mechanism (e.g., contraverifying that the organization's requirement control have been met by all appropriate corproviders, and third parties. Assign responsi with those contractors, service providers, an staff members.	ts for physical access ntractors, service bility for working directly	Verification
Implement an <i>informal</i> mechanism (e.g., assigning that the organization's requirement control have been met by all appropriate conproviders, and third parties. Assign responsitions with those contractors, service providers, and staff members.	its for physical access intractors, service ibility for working directly	Verification

Candidate Mitigation Activities	7. Physical Access Control
Mitigation Activity	Protection Strategy Link
Develop procedures for controlling physical access to	
the building and premises	
selected work areas	
IT hardware	
software media	
• other	
Rearrange office/work spaces to restrict physical access to systems, computers, or other devices by unauthorized personnel.	
Implement sign-in sheets to manage visitors' access to the building and/or designated work areas.	
Implement card access to restrict physical access to the building.	
Implement card access to restrict physical access to specific work areas.	
Replace door locks in specific work areas.	
Retain the services of security guards to protect the premises.	
Rearrange the physical setup of computing equipment in specific areas to counteract environmental threats.	
Perform an audit of physical security to identify security weaknesses in the physical infrastructure.	
Develop procedures for specific systems defining the designated time that a device can remain logged on before that device is automatically locked or logged off.	-
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for controlling physical access in the organization and to verify that those requirements have been met.	

8. Monitoring and Auditing Physical Security		Candidate Mitigation Activities
Mitigation Activity		Protection Strategy Link
Change responsibility for keeping maintenance records that document repairs and modifications to IT hardware.		Responsibility
Change responsibility for monitoring physical accordance	ess to controlled IT	Responsibility
Change responsibility for monitoring physical accessoftware media.	ess to controlled IT	Responsibility
Change responsibility for monitoring physical account work areas.	ess to restricted	Responsibility
Change responsibility for reviewing monitoring rebasis.	cords on a periodic	Responsibility
Change responsibility for investigating and addres activity that is identified.	sing any unusual	Responsibility
Document formal procedures for monitoring physical building and premises, work areas, IT hardware, a	ical access to the nd software media.	Procedures
Send selected staff members to training for monitoring physical access to the building and premises, work areas, IT hardware, and software media.		Training
Implement a <i>formal</i> mechanism (e.g., contract mechanism) for communicating the organization's requirements for monitoring physical security to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Collaborative Issues
Implement an <i>informal</i> mechanism (e.g., assign responsibility) for communicating the organization's requirements for monitoring physical security to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Collaborative Issues
Implement a <i>formal</i> mechanism (e.g., contract mechanism) for verifying that the organization's requirements for monitoring physical security have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Verification
Implement an <i>informal</i> mechanism (e.g., assign responsibility) for verifying that the organization's requirements for monitoring physical security have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Verification

Candidate Mitigation Activities

8. Monitoring and Auditing Physical Security

Mitigation Activity	Protection Strategy Link
Install video cameras in designated areas of the premises.	
Retain the services of security guards to monitor activity on the premises.	
Implement sign-in sheets to log visitors' access to the building and/or designated work areas.	
Implement card access to log physical access to the building and/or designated work areas.	
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for monitoring physical security in the organization and to verify that those requirements have been met.	·

9. System and Network Management	Candidate Mitigation Activities	
Mitigation Activity		Protection Strategy Link
Change responsibility for configuring IT hardware and software.		Responsibility
Change responsibility for securely storing se backups stored off site, process for discarding	ensitive information (e.g., ag sensitive information).	Responsibility
Change responsibility for checking the integ	rity of installed software.	Responsibility
Change responsibility for keeping systems u revisions, patches, and recommendations in	p to date with respect to security advisories.	Responsibility
Change responsibility for making and tracki hardware and software.	ng changes to IT	Responsibility
Change responsibility for managing passworprivileges.	rds, accounts, and	Responsibility
Change responsibility for selecting system a tools.	nd network management	Responsibility
Document formal procedures for managing	systems and networks.	Procedures
Send selected staff members to training for managing systems and networks.		Training
Implement a <i>formal</i> mechanism (e.g., contract mechanism) for communicating the organization's requirements for secure system and network management to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Collaborative Issues
Implement an <i>informal</i> mechanism (e.g., assign responsibility) for communicating the organization's requirements for secure system and network management to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Collaborative Issues
Implement a <i>formal</i> mechanism (e.g., contract mechanism) for verifying that the organization's requirements for secure system and network management have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Verification
Implement an <i>informal</i> mechanism (e.g., as verifying that the organization's requirement network management have been met by all service providers, and third parties. Assign directly with those contractors, service providered staff members.	appropriate contractors, responsibility for working	Verification

Candidate Mitigation Activities

9. System and Network Management

Mitigation Activity	Protection Strategy Link
Check the configuration of IT hardware and software on specific systems.	
Check the integrity of installed software on specific systems.	
Check specific systems to ensure that they are up to date with respect to revisions, patches, and recommendations in security advisories.	
Check specific systems for default accounts and accounts that are no longer used.	
Check specific systems for easy-to-crack passwords.	
Check specific systems to see if they are running unnecessary services.	
Check specific systems for the presence of viruses or other malicious code.	·
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for securely managing systems and networks in the organization and to verify that those requirements have been met.	

10. Monitoring and Auditing IT Security		Candidate Mitigation Activities
Mitigation Activity		Protection Strategy Link
Change responsibility for using system and r to track system and network activity.	network monitoring tools	Responsibility
Change responsibility for periodically auditing security components for compliance with po	ng the firewall and other licy.	Responsibility
Change responsibility for investigating and a activity that is identified.	ddressing any unusual	Responsibility
Document formal procedures for monitoring systems and networks.	network access to	Procedures
Send selected staff members to training for r to systems and networks.	nonitoring network access	Training
Implement a <i>formal</i> mechanism (e.g., contra communicating the organization's requirement security to all appropriate contractors, service parties. Assign responsibility for working discontractors, service providers, and third partimembers.	ents for monitoring IT e providers, and third irectly with those	Collaborative Issues
Implement an <i>informal</i> mechanism (e.g., assign responsibility) for communicating the organization's requirements for monitoring IT security to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Collaborative Issues
Implement a <i>formal</i> mechanism (e.g., contract mechanism) for verifying that the organization's requirements for monitoring IT security have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Verification
Implement an <i>informal</i> mechanism (e.g., ass verifying that the organization's requiremen security have been met by all appropriate coproviders, and third parties. Assign responsi with those contractors, service providers, an staff members.	ts for monitoring IT ontractors, service bility for working directly	Verification

Candidate Mitigation Activities

10. Monitoring and Auditing IT Security

Mitigation Activity	Protection Strategy Link
Develop procedures for	
 reviewing system logs 	
 using system and network monitoring tools to track system activity 	
 auditing the firewall and other security components periodically for compliance with policy 	
 investigating and addressing any unusual activity that is identified 	
Implement an intrusion detection system and assign an IT staff member the responsibility of tracking network activity.	
Perform an audit of the firewall and other security components to ensure that they are compliant with the organization's security policies.	
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for monitoring IT security in the organization and to verify that those requirements have been met.	

11. Authentication and Authorization	Candidate Mitigation Activities	
Mitigation Activity		Protection Strategy Link
Change responsibility for implementing access controls (e.g., file permissions, network configuration) to restrict user access to information, sensitive systems, specific applications and services, and network connections.		Responsibility
Change responsibility for implementing user passwords, biometrics) to restrict user access systems, specific applications and services, a	s to information, sensitive	Responsibility
Change responsibility for establishing and te systems and information for both individuals	erminating access to s and groups.	Responsibility
Document formal procedures for restricting user access to information, sensitive systems, specific applications and services, and network connections.		Procedures
Send selected staff members to training for implementing technological measures to restrict user access to information, sensitive systems, specific applications and services, and network connections.		Training
Implement a <i>formal</i> mechanism (e.g., contract mechanism) for communicating the organization's requirements for controlling access to systems and information to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Collaborative Issues
Implement an <i>informal</i> mechanism (e.g., assign responsibility) for communicating the organization's requirements for controlling access to systems and information to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Collaborative Issues
Implement a <i>formal</i> mechanism (e.g., contract mechanism) for verifying that the organization's requirements for controlling access to systems and information have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Verification
Implement an <i>informal</i> mechanism (e.g., assistant verifying that the organization's requirement systems and information have been met by a service providers, and third parties. Assign directly with those contractors, service proviselected staff members.	all appropriate contractors, responsibility for working	Verification

Candidate Mitigation Activities 11. Authentication and Authorization Mitigation Activity Protection Strategy Link Check access controls (e.g., file permissions, network configuration) on specific systems. -- Check that appropriate authentication mechanisms (e.g., passwords, biometrics) are used to restrict user access to specific systems. -- Check specific systems for easy-to-crack passwords. -- Check specific systems to ensure that all devices that access those systems automatically timeout after a designated period of time. -- Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for controlling access to systems and information in the organization and to verify that those requirements have been met. --

12. Vulnerability Management		Candidate Mitigation Activities
Mitigation Activity		Protection Strategy Link
Change responsibility for selecting vulnerability checklists, and scripts.	lity evaluation tools,	Responsibility
Change responsibility for scheduling and per vulnerability evaluations on a periodic basis.	forming technology	Responsibility
Change responsibility for keeping up to date types and attack methods.	with known vulnerability	Responsibility
Change responsibility for reviewing sources vulnerability announcements, security alerts,	of information on and notices.	Responsibility
Change responsibility for interpreting the result vulnerability evaluations.	sults of technology	Responsibility
Change responsibility for addressing technol are identified.	ogy vulnerabilities that	Responsibility
Change responsibility for maintaining secure of technology vulnerability data.	e storage and disposition	Responsibility
Document formal procedures for managing	echnology vulnerabilities.	Procedures
Send selected staff members to training for managing technology vulnerabilities.		Training
Implement a <i>formal</i> mechanism (e.g., contract mechanism) for communicating the organization's requirements for managing technology vulnerabilities to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Collaborative Issues
Implement an <i>informal</i> mechanism (e.g., assign responsibility) for communicating the organization's requirements for managing technology vulnerabilities to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Collaborative Issues
Implement a <i>formal</i> mechanism (e.g., contract mechanism) for verifying that the organization's requirements for managing technology vulnerabilities have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Verification
Implement an <i>informal</i> mechanism (e.g., assigning that the organization's requirement technology vulnerabilities have been met by contractors, service providers, and third parties to selected staff members.	ats for managing all appropriate ties. Assign responsibility	Verification

Candidate Mitigation Activities	12. Vulnerability Management
Mitigation Activity	Protection Strategy Link
Check specific systems for technology vulnerabilities.	
Perform an audit of information technology security to identify security weaknesses in the computing infrastructure.	
Contract with an outside organization to attack your organization's systems and network via the Internet (i.e., penetration testing, red team).	
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for managing technology vulnerabilities in the organization and to verify that those requirements have been met.	

13. Encryption		Candidate Mitigation Activities
Mitigation Activity		Protection Strategy Link
Change responsibility for implementing encryption technologies to protect sensitive information that is electronically stored and transmitted (e.g., data encryption, public key infrastructure, virtual private network technology).		Responsibility
Change responsibility for implementing encr remotely managing systems, routers, and fire	ypted protocols for ewalls.	Responsibility
Change responsibility for implementing encr remotely managing systems, routers, and fire	ypted protocols for ewalls.	Responsibility
Document formal procedures for implementitechnologies.	ng and using encryption	Procedures
Send selected IT staff members to training for encryption technologies.	or implementing	Information Technology Staff Training
Send selected staff members to training for u technologies.	ising encryption	Staff Training
Implement a formal mechanism (e.g., contracommunicating the organization's requirement sensitive information to all appropriate contract and third parties. Assign responsibility for withose contractors, service providers, and third members.	ents for protecting ractors, service providers, vorking directly with	Collaborative Issues
Implement an <i>informal</i> mechanism (e.g., ass communicating the organization's requirement sensitive information to all appropriate contrand third parties. Assign responsibility for values those contractors, service providers, and thir members.	ents for protecting ractors, service providers, working directly with	Collaborative Issues
Implement a <i>formal</i> mechanism (e.g., contra verifying that the organization's requirement information have been met by all appropriate providers, and third parties. Assign responsitivith those contractors, service providers, and staff members.	ts for protecting sensitive e contractors, service bility for working directly	Verification
Implement an <i>informal</i> mechanism (e.g., ass verifying that the organization's requirement information have been met by all appropriate providers, and third parties. Assign responsitivith those contractors, service providers, and staff members.	ts for protecting sensitive e contractors, service bility for working directly	Verification

Candidate Mitigation Activities	13. Encryption	
Mitigation Activity	Protection Strategy Link	
Implement encryption technologies to protect specific types of information and/or systems.		
Arrange a meeting with all appropriate contractors, service provide and third parties to communicate requirements for protecting sensit information in the organization and to verify that those requirement have been met.	tive	

14. Security Architecture and Design		Candidate Mitigation Activities
Mitigation Activity		Protection Strategy Link
Change responsibility for designing security revised systems and networks.	controls in new and	Responsibility
Change responsibility for documenting and reshow the enterprise-wide security architecture	evising diagrams that e and network topology.	Responsibility
Document formal security architecture and de	esign practices.	Procedures
Send selected staff members to training for d and networks.	esigning secure systems	Training
Implement a <i>formal</i> mechanism (e.g., contract communicating the organization's requirement appropriate security features into systems and appropriate contractors, service providers, and responsibility for working directly with those providers, and third parties to selected staff in	nts for incorporating d networks to all d third parties. Assign c contractors, service	Collaborative Issues
Implement an <i>informal</i> mechanism (e.g., assign responsibility) for communicating the organization's requirements for incorporating appropriate security features into systems and networks to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Collaborative Issues
Implement a <i>formal</i> mechanism (e.g., contract mechanism) for verifying that the organization's requirements for incorporating appropriate security features into systems and networks have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.		Verification
Implement an <i>informal</i> mechanism (e.g., ass verifying that the organization's requirement appropriate security features into systems an by all appropriate contractors, service provide Assign responsibility for working directly we service providers, and third parties to selecte	ts for incorporating d networks have been met lers, and third parties. ith those contractors,	Verification

Candidate Mitigation Activities	14. Security Architecture and Design
Mitigation Activity	Protection Strategy Link
Update the design of specific systems to include appropriate secu controls.	rity
Investigate periodic crashes of specific systems and correct any d problems that lead to those crashes.	esign
Document or update diagrams that show the enterprise-wide secu architecture and network topology.	rity
Arrange a meeting with all appropriate contractors, service provide and third parties to communicate requirements for incorporating appropriate security features into systems and networks and to vethat those requirements have been met.	

15. Incident Management		Candidate Mitigation Activities
Mitigation Activity		Protection Strategy Link
Change responsibility for documenting and ridentifying, reporting, and responding to sus and violations.	revising procedures for pected security incidents	Responsibility
Change responsibility for documenting and r procedures for working with law enforcement	revising policies and nt agencies.	Responsibility
Change responsibility for testing incident mage a periodic basis.	anagement procedures on	Responsibility
Document formal procedures for managing i	incidents.	Procedures
Send selected staff members to training for r	nanaging incidents.	Training
Implement a <i>formal</i> mechanism (e.g., contracommunicating the organization's requirement incidents to all appropriate contractors, service parties. Assign responsibility for working discontractors, service providers, and third part members.	ents for managing ice providers, and third irectly with those	Collaborative Issues
Implement an <i>informal</i> mechanism (e.g., ass communicating the organization's requirement incidents to all appropriate contractors, service parties. Assign responsibility for working do contractors, service providers, and third partimembers.	ents for managing ice providers, and third irectly with those	Collaborative Issues
Implement a <i>formal</i> mechanism (e.g., contraverifying that the organization's requirementave been met by all appropriate contractors third parties. Assign responsibility for work contractors, service providers, and third partimembers.	ts for managing incidents s, service providers, and ing directly with those	Verification
Implement an <i>informal</i> mechanism (e.g., assignifying that the organization's requirement have been met by all appropriate contractors third parties. Assign responsibility for work contractors, service providers, and third partimembers.	its for managing incidents s, service providers, and ing directly with those	Verification

Candidate Mitigation Activities	15. Incident Management
Mitigation Activity	Protection Strategy Link
Test current incident management procedures.	
Arrange a meeting with all appropriate contractors, service provide and third parties to communicate requirements for managing incide in the organization and to verify that those requirements have been met.	lents

6 Mitigation Plan Worksheet

Phase 3 Process S5 Activity S5.3

Step 28

Develop mitigation plans for each security practice area selected during Step 27.

As you complete this step, if you have difficulty coming up with potential mitigation activities for a security practice area, review examples of mitigation activities for that area in the *Mitigation Activities Guide*.

Rationale
Why did you select each activity?

Mitigation Responsibility	Additional Support
Who needs to be involved in implementing each activity? Why?	What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?
·	

Mitigation Area:	

Step 28	
Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	Why did you select each activity?
	·
	·
	·
•	

Mitigation Responsibility	Additional Support
Who needs to be involved in implementing each activity? Why?	What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?
	·
·	
·	

Mitigation Area:		
Rationale		
Why did you select each activity?		
,		

Mitigation Responsibility	Additional Support
Who needs to be involved in implementing each activity? Why?	What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?
)
·	
·	
·	

Mitigation Area: _	
--------------------	--

Step 28	
Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	Why did you select each activity?
	·
	·

Mitigation Responsibility	Additional Support
Who needs to be involved in implementing each activity? Why?	What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?
·	

Mitigation Areas	

Step 28	
Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	Why did you select each activity?

Mitigation Responsibility	Additional Support			
Who needs to be involved in implementing each activity? Why?				
•				
	·			
•				
•				

Mitigation Area: _	
--------------------	--

litigation Activity	Rationale	
Vhich mitigation activities are you going to implement in this ecurity practice area?	Why did you select each activity?	
		PASSANIPARAMA
		,essential river
•		
		•

Mitigation Responsibility	Additional Support
Who needs to be involved in implementing each activity? Why?	What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?
·	

7 Next Steps Worksheet

Phase 3
Process S5
Activity S5.5

Step 30

Determine what your organization must do to implement the results of this evaluation and improve its security posture.

Step 30

Management Sponsorship for Security Improvement

What must management do to support the implementation of OCTAVE-S results?

Consider the following:

- Contribute funds to information security activities.
- Assign staff to information security activities.
- Ensure that staff members have sufficient time allocated to information security activities.
- Enable staff to receive training about information security.
- Make information security a strategic priority.

Monitoring Implementation
What will the organization do to track progress and ensure that the results of this evaluation are implemented?
Expanding the Current Information Security Risk Evaluation
Will you expand the current OCTAVE-S evaluation to include additional critical assets? Which ones?
Next Information Committy Dick Evolution
Next Information Security Risk Evaluation When will the organization conduct its next OCTAVE-S evaluation?
when will the organization conduct as next octive a continuation.

REPORT DOC	CUMENTATION	N PAGE	OMB N	Approved No. 0704-0188
Public reporting burden for this collection existing data sources, gathering and ma this burden estimate or any other aspect Services, Directorate for information Op- Management and Budget, Paperwork Ri	intaining the data needed, and completi t of this collection of information, includii erations and Reports, 1215 Jefferson Di	ing and reviewing the colle ng suggestions for reducir avis Highway, Suite 1204,	o this burden, to	Washington Headquarters
1. AGENCY USE ONLY	2. REPORT DATE		3. REPORT T	YPE AND DATES COVERED
(Leave Blank)	January 2005		Final	
4. TITLE AND SUBTITLE			5. FUNDING	NUMBERS
OCTAVE-S Implementation	on Guide, Version 1.0, Volum	ne 9	F19628	-00-C-0003
6. AUTHOR(S)				
Christopher Alberts, Audr	rey Dorofee, James Stevens,	Carol Woody		
7. PERFORMING ORGANIZATION NAM	ME(S) AND ADDRESS(ES)			ING ORGANIZATION
Software Engineering Ins	titute		REPORT N	
Carnegie Mellon Universi Pittsburgh, PA 15213	ity		CIVIU/S	EI-2003-HB-003
9. SPONSORING/MONITORING AGENC	CY NAME(S) AND ADDRESS(ES)			ING/MONITORING AGENCY
HQ ESC/XPK			REPORT N	IUMBER
5 Eglin Street	4 0440			
Hancom AER MA 0173	1-2116			
Hanscom AFB, MA 0173	1-2116			
Hanscom AFB, MA 0173 11. SUPPLEMENTARY NOTES	1-2116			
Hanscom AFB, MA 0173	-		128 DISTRIBU	TION CODE
Hanscom AFB, MA 0173 11. SUPPLEMENTARY NOTES	TEMENT		12B DISTRIBU	TION CODE
Hanscom AFB, MA 0173 11. SUPPLEMENTARY NOTES 12. DISTRIBUTION/AVAILABILITY STAT Unclassified/Unlimited, D 13. ABSTRACT (MAXIMUM 200 WORD	TEMENT DTIC, NTIS (S)			
Hanscom AFB, MA 0173 11. SUPPLEMENTARY NOTES 12. DISTRIBUTION/AVAILABILITY STAT Unclassified/Unlimited, D 13. ABSTRACT (MAXIMUM 200 WORD The Operationally Critica	TEMENT OTIC, NTIS Is) Il Threat, Asset, and Vulnerab	oility Evaluation SM (OCTAVE®) (approach defines a ris
Hanscom AFB, MA 0173 11. SUPPLEMENTARY NOTES 12. DISTRIBUTION/AVAILABILITY STATE Unclassified/Unlimited, D 13. ABSTRACT (MAXIMUM 200 WORD The Operationally Critical based strategic assessm	TEMENT OTIC, NTIS IS) Il Threat, Asset, and Vulnerablent and planning technique fo	or security. OCTAV	OCTAVE®) (E is a self-d	approach defines a ris
Hanscom AFB, MA 0173 11. SUPPLEMENTARY NOTES 12A DISTRIBUTION/AVAILABILITY STAT Unclassified/Unlimited, D 13. ABSTRACT (MAXIMUM 200 WORD The Operationally Critica based strategic assessm meaning that people from	TEMENT OTIC, NTIS IS) I Threat, Asset, and Vulnerablent and planning technique for an organization assume res	or security. OCTAV sponsibility for setti	OCTAVE®) (I'E is a self-ding the organ	approach defines a ris lirected approach, nization's security
Hanscom AFB, MA 0173 11. SUPPLEMENTARY NOTES 12. DISTRIBUTION/AVAILABILITY STATE Unclassified/Unlimited, D 13. ABSTRACT (MAXIMUM 200 WORD The Operationally Critical based strategic assessm meaning that people from strategy, OCTAVE-S is a	TEMENT OTIC, NTIS IS) I Threat, Asset, and Vulnerablent and planning technique for an organization assume responses to variation of the approach tai	or security. OCTAV sponsibility for setting flored to the limited	OCTAVE®) (E is a self-ding the organ means and	approach defines a ris lirected approach, nization's security unique constraints
Hanscom AFB, MA 0173 11. SUPPLEMENTARY NOTES 12. DISTRIBUTION/AVAILABILITY STAT Unclassified/Unlimited, D 13. ABSTRACT (MAXIMUM 200 WORD The Operationally Critica based strategic assessm meaning that people from strategy. OCTAVE-S is a typically found in small of	TEMENT OTIC, NTIS OS) Il Threat, Asset, and Vulnerablent and planning technique for an organization assume residuation of the approach tairganizations (less than 100 progenizations)	or security. OCTAV sponsibility for setti flored to the limited eople). OCTAVE-S	OCTAVE®) a 'E is a self-orger means and is led by a	approach defines a ris lirected approach, nization's security unique constraints small, interdisciplinary
Hanscom AFB, MA 0173 11. SUPPLEMENTARY NOTES 12. DISTRIBUTION/AVAILABILITY STAT Unclassified/Unlimited, D 13. ABSTRACT (MAXIMUM 200 WORD The Operationally Critica based strategic assessm meaning that people from strategy. OCTAVE-S is a typically found in small of team (three to five people)	TEMENT OTIC, NTIS IS IS IS Threat, Asset, and Vulnerablent and planning technique for an organization assume result variation of the approach tail reganizations (less than 100 poet) of an organization's persor	or security. OCTAV sponsibility for setti lored to the limited eople). OCTAVE-S nnel who gather an	OCTAVE®) (if is a self-ong the organ means and is led by a side analyze in	approach defines a ris lirected approach, nization's security unique constraints small, interdisciplinary formation, producing
Hanscom AFB, MA 0173 11. SUPPLEMENTARY NOTES 12. DISTRIBUTION/AVAILABILITY STATE Unclassified/Unlimited, D 13. ABSTRACT (MAXIMUM 200 WORD The Operationally Critical based strategic assessm meaning that people from strategy. OCTAVE-S is a typically found in small of team (three to five people protection strategy and m	TEMENT OTIC, NTIS Is) Il Threat, Asset, and Vulnerablent and planning technique for an organization assume resit variation of the approach tail rganizations (less than 100 poe) of an organization's personnitigation plans based on the	or security. OCTAV sponsibility for setting lored to the limited eople). OCTAVE-Sanel who gather an organization's unique.	OCTAVE®) and the organ means and is led by a sed analyze in ue operation	approach defines a ris lirected approach, nization's security unique constraints small, interdisciplinary formation, producing nal security risks. To
Hanscom AFB, MA 0173 11. SUPPLEMENTARY NOTES 12. DISTRIBUTION/AVAILABILITY STATE Unclassified/Unlimited, D 13. ABSTRACT (MAXIMUM 200 WORD The Operationally Critical based strategic assessm meaning that people from strategy. OCTAVE-S is a typically found in small of team (three to five people protection strategy and m conduct OCTAVE-S effect	TEMENT OTIC, NTIS as) I Threat, Asset, and Vulnerablent and planning technique for an organization assume reseavariation of the approach tairganizations (less than 100 pe) of an organization's personnitigation plans based on the ctively, the team must have be	or security. OCTAV sponsibility for setting lored to the limited eople). OCTAVE-Sonel who gather an organization's uniquoad knowledge of	OCTAVE®) and the organ means and is led by a sed analyze in ue operation	approach defines a ris lirected approach, nization's security unique constraints small, interdisciplinary formation, producing nal security risks. To
Hanscom AFB, MA 0173 11. SUPPLEMENTARY NOTES 12. DISTRIBUTION/AVAILABILITY STATE Unclassified/Unlimited, D 13. ABSTRACT (MAXIMUM 200 WORD The Operationally Critical based strategic assessm meaning that people from strategy. OCTAVE-S is a typically found in small of team (three to five people protection strategy and m conduct OCTAVE-S effect	TEMENT OTIC, NTIS Is) Il Threat, Asset, and Vulnerablent and planning technique for an organization assume resit variation of the approach tail rganizations (less than 100 poe) of an organization's personnitigation plans based on the	or security. OCTAV sponsibility for setting lored to the limited eople). OCTAVE-Sonel who gather an organization's uniquoad knowledge of	OCTAVE®) and the organ means and is led by a sed analyze in ue operation	approach defines a ris lirected approach, nization's security unique constraints small, interdisciplinary formation, producing nal security risks. To ation's business and
Hanscom AFB, MA 0173 11. SUPPLEMENTARY NOTES 12. DISTRIBUTION/AVAILABILITY STATE Unclassified/Unlimited, D 13. ABSTRACT (MAXIMUM 200 WORD The Operationally Critical based strategic assessm meaning that people from strategy. OCTAVE-S is a typically found in small of team (three to five people protection strategy and meaning that conduct OCTAVE-S effects security processes, so it	TEMENT OTIC, NTIS Is) Il Threat, Asset, and Vulnerablent and planning technique for an organization assume resit variation of the approach tairganizations (less than 100 pe) of an organization's personnitigation plans based on the ctively, the team must have be will be able to conduct all act	or security. OCTAV sponsibility for setting lored to the limited eople). OCTAVE-Sonel who gather an organization's uniquoad knowledge of	OCTAVE®) and the organ means and is led by a self analyze in the organize the organizers.	approach defines a ris lirected approach, nization's security unique constraints small, interdisciplinary formation, producing nal security risks. To ation's business and
Hanscom AFB, MA 0173 11. SUPPLEMENTARY NOTES 12. DISTRIBUTION/AVAILABILITY STATE Unclassified/Unlimited, D 13. ABSTRACT (MAXIMUM 200 WORD The Operationally Critical based strategic assessm meaning that people from strategy. OCTAVE-S is a typically found in small of team (three to five people protection strategy and in conduct OCTAVE-S effect security processes, so it	TEMENT OTIC, NTIS Is) Il Threat, Asset, and Vulnerablent and planning technique for an organization assume resit variation of the approach tairganizations (less than 100 pe) of an organization's personnitigation plans based on the ctively, the team must have be will be able to conduct all act	or security. OCTAV sponsibility for setting lored to the limited eople). OCTAVE-Sonel who gather an organization's uniquoad knowledge of	OCTAVE®) and the organ means and is led by a side analyze in the organization the organization of the orga	approach defines a ris lirected approach, nization's security unique constraints small, interdisciplinary formation, producing nal security risks. To ation's business and
Hanscom AFB, MA 0173 11. SUPPLEMENTARY NOTES 12. DISTRIBUTION/AVAILABILITY STATE Unclassified/Unlimited, D 13. ABSTRACT (MAXIMUM 200 WORD The Operationally Critical based strategic assessm meaning that people from strategy. OCTAVE-S is a typically found in small of team (three to five people protection strategy and m conduct OCTAVE-S effect security processes, so it 14. SUBJECT TERMS information security, risk	TEMENT OTIC, NTIS Is) Il Threat, Asset, and Vulnerablent and planning technique for an organization assume resit variation of the approach tairganizations (less than 100 pe) of an organization's personnitigation plans based on the ctively, the team must have be will be able to conduct all act	or security. OCTAV sponsibility for setting lored to the limited eople). OCTAVE-Sonel who gather an organization's uniquoad knowledge of	OCTAVE®) and the organ means and is led by a side analyze in the organization the organization of the orga	approach defines a ris lirected approach, nization's security unique constraints small, interdisciplinary formation, producing nal security risks. To ation's business and
Hanscom AFB, MA 0173 11. SUPPLEMENTARY NOTES 12. DISTRIBUTION/AVAILABILITY STATE Unclassified/Unlimited, D 13. ABSTRACT (MAXIMUM 200 WORD The Operationally Critical based strategic assessm meaning that people from strategy. OCTAVE-S is a typically found in small of team (three to five people protection strategy and in conduct OCTAVE-S effer security processes, so it 14. SUBJECT TERMS information security, risk 16. PRICE CODE	TEMENT OTIC, NTIS Is) Il Threat, Asset, and Vulnerablent and planning technique for an organization assume resit variation of the approach tairganizations (less than 100 pe) of an organization's personnitigation plans based on the ctively, the team must have be will be able to conduct all act	or security. OCTAV sponsibility for setting lored to the limited eople). OCTAVE-Sonel who gather an organization's uniquoad knowledge of	OCTAVE®) and the organ means and is led by an analyze in the organization. 15. NUMBER 132	approach defines a ris lirected approach, nization's security unique constraints small, interdisciplinary formation, producing nal security risks. To ation's business and